2021-03

NORMALIZING CYBERSECURITY: IMPROVING CYBER INCIDENT RESPONSE WITH THE INCIDENT COMMAND SYSTEM

Hanson, Darin T.

Monterey, CA; Naval Postgraduate School

http://hdl.handle.net/10945/67133

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NORMALIZING CYBERSECURITY:
IMPROVING CYBER INCIDENT RESPONSE
WITH THE INCIDENT COMMAND SYSTEM

by

Darin T. Hanson

March 2021

Co-Advisors:	Glen L. Woodbury Lauren S. Fernandez (contractor)

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2021	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE NORMALIZING CYBERSECURITY: IMPROVING CYBER INCIDENT RESPONSE WITH THE INCIDENT COMMAND SYSTEM	**5. FUNDING NUMBERS**
6. AUTHOR(S) Darin T. Hanson	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In 2018, the Colorado Department of Transportation was hit with a ransomware attack that resulted in the first-ever state emergency declaration for a cyber attack. Cyber attacks against the nation and its infrastructure are expected to increase, yet no extensive research exists on the United States’ designated response framework for them. This thesis investigated the application of the Incident Command System (ICS) in significant cyber incidents and how the system may be improved for these events. A mixed method study consisting of case studies, senior leader interviews, and a quantitative survey was used to evaluate ICS specific to the framework’s eight core concepts. The research includes findings on variables that impact the effectiveness of response frameworks in cyber events. Recommendations are made to improve cyber response.

14. SUBJECT TERMS Incident Command System, ICS, National Incident Management System, NIMS, cyber response, cybersecurity, survey, interview, case study, ransomware, significant cyber incident, core concept	**15. NUMBER OF PAGES** 153
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

NORMALIZING CYBERSECURITY: IMPROVING CYBER INCIDENT RESPONSE WITH THE INCIDENT COMMAND SYSTEM

Darin T. Hanson
Critical Infrastructure Program Manager,
North Dakota Department of Emergency Services
BS, University of Mary, 2009
MBA, University of Mary, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2021

Approved by: Glen L. Woodbury
Co-Advisor

Lauren S. Fernandez
Co-Advisor

Erik J. Dahl
Associate Professor,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2018, the Colorado Department of Transportation was hit with a ransomware attack that resulted in the first-ever state emergency declaration for a cyber attack. Cyber attacks against the nation and its infrastructure are expected to increase, yet no extensive research exists on the United States' designated response framework for them. This thesis investigated the application of the Incident Command System (ICS) in significant cyber incidents and how the system may be improved for these events. A mixed method study consisting of case studies, senior leader interviews, and a quantitative survey was used to evaluate ICS specific to the framework's eight core concepts. The research includes findings on variables that impact the effectiveness of response frameworks in cyber events. Recommendations are made to improve cyber response.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
ANOM	Analysis of Means
CDOT	Colorado Department of Transportation
CISO	Chief Information Security Officer
EM/HS	Emergency Management/Homeland Security
EMAC	Emergency Management Assistance Compact
ICS	Incident Command System
IRB	Institutional Review Board
IT/CS	Information Technology/Cybersecurity
M	Mean
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
OIT	Office of Information Technology
SEOC	State Emergency Operations Center

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

In February of 2018, the state of Colorado became the first state in the nation to issue an emergency declaration for a cyber attack after its Department of Transportation was struck with ransomware.[1] After early struggles responding to the incident, the Incident Command System (ICS) was implemented and a Unified Command was established with promising results.[2] With the expectation that the adversaries of the United States will continue to expand their adoption of cyber attacks "to steal information, to influence our citizens, or to disrupt critical infrastructure," both Emergency Management/Homeland Security (EM/HS) and Information Technology/Cyber Security (IT/CS) professionals should be preparing for significant cyber incidents.[3] This thesis investigated the application of ICS in response to significant cyber incidents and how it can be improved. To accomplish this, a mixed method study consisting of case studies, qualitative senior leader interviews, and a quantitative survey was conducted. The analysis centered around the eight core concepts of ICS: common terminology, integrated communications, modular organization, recognized command structure, manageable supervisory structure, consolidated action plans, comprehensive resource management, and pre-designated facilities.

The first, and simple, conclusion of this thesis is that ICS is applicable in a significant cyber incident response. The findings of the case studies and senior leader interviews showed that ICS does indeed have a place when responding to cyber incidents beyond the routine cyber emergencies that IT/CS professionals deal with frequently. The framework is already standard in EM/HS, providing a large pool of trained personnel and opportunities for free Federal Emergency Management Agency (FEMA) training on the

[1] Colorado Department of Transportation, *CDOT Cyber Incident: After-Action Report* (Denver: Colorado Department of Transportation, 2018), 3, https://www.colorado.gov/pacific/dhsem/atom/129636.

[2] Colorado Department of Transportation, 3.

[3] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

framework.[4] Conversely, there are still few IT/CS practitioners trained on ICS and some past natural disaster responses where the framework was used with poor results.[5] There is opportunity for improvement in the implementation of ICS while maintaining the core concepts praised by practitioners.[6]

The research provides important insight into how the eight core concepts of ICS relate to significant cyber incident response.

- There were strong indications that a lack of **common terminology** across the professional fields of responders is an issue. While the quantitative survey analysis indicated that IT/CS responders believed their organizations were using common terminology better than their EM/HS counterparts, the qualitative findings suggested that the EM/HS group did not understand the technical terminology, which can be a hindrance during incident response.

- **Integration of communications** was another concept with conflicting findings. Quantitative survey results revealed that the IT/CS group rated their organizations highly, but qualitative interview findings indicated that integrated communications were a potential weakness in response efforts due to networks being impacted during a cyber attack.

- The application of the **modular organization** concept was rated high by the surveyed EM/HS practitioners and the case studies and interviews suggested

[4] John R. Harrald, "Agility and Discipline: Critical Success Factors for Disaster Response," *Annals of the American Academy of Political and Social Science* 604, no. 1 (2006): 263, https://doi.org/10.1177/0002716205285404.

[5] Dick A. Buck, Joseph E. Trainor, and Benigno E. Aguirre, "A Critical Evaluation of the Incident Command System and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006), https://doi.org/10.2202/1547-7355.1252.

[6] Ronald W. Perry, "Incident Management Systems in Disaster Management," *Disaster Prevention and Management: An International Journal* 12, no. 5 (2003): 411, https://doi.org/10.1108/09653560310507226; Hank Christen et al., "An Overview of Incident Management Systems," *Perspectives on Preparedness*, no. 4 (2001): 6; Gregory Bigley and Karlene Roberts, "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments," *Academy of Management Journal* 44, no. 6 (2001): 1283; and Brian Bennett, "Effective Emergency Management: A Closer Look at the Incident Command System," *Professional Safety* 56, no. 11 (November 2011): 31, ProQuest.

that ICS provides a useful structure for the systematic expansion and contraction of response resources.

- Both the EM/HS and IT/CS groups rated their organizations' use of the **recognized command structure** relatively high while the interviews supported a need for a collaborative command structure, which may best be instituted using an ICS framework.
- The concept of **manageable supervisory structure** was rated low in application by both groups while the findings suggested that in a cyber incident response the technology used in information systems and integrated technologies resulted in a lower importance of the concept during response activities.
- The concepts of **consolidated action plans** and **comprehensive resource management** revealed an important link in the research due to the limited technical cyber response resources and the need to provide consolidated action plans to prioritize the limited resources usage. The EM/HS group rated their organizations higher in both the comprehensive resource management and consolidated action plans concepts while the findings supported the use of the ICS framework to improve incident response relative to both concepts.
- Finally, the concept of **pre-designated facilities** showed the IT/CS group rated their organizations higher for implementation while the interviews suggested a need for multiple pre-designated response locations, an off-site location for coordinating second and third order effects, and one or more locations where the technical cyber response will occur.

Implications and improvements for each area are discussed in the thesis.

This thesis also draws two important conclusions from the results of the quantitative analysis. First, the survey results showed that prior response experience to significant cyber incidents raised the perceptions of organizations' application of each of the core concepts. The research attributes this to experiential learning. Second, the survey results also indicated that those with less than five-years of experience rated their organizations higher in application of each core concept, which the research attributes to an over-confidence by the less experienced practitioners. These two findings have important implications for improvement in the implementation of ICS.

This thesis made five recommendations:

- *Implement ICS in Significant Cyber Incidents:* Implementing ICS in these events could assist entities to integrate communications across the response body, provide structure to the expansion and contraction of response assets, unify objectives and strategies of response stakeholders, and prioritize and comprehensively manage response resources.
- *Include Cross Training & Collaborative Exercise:* Rather than wait for an incident to occur, the implementation of cross-training between EM/HS and IT/CS practitioners with follow-on collaborative response exercises would help to establish common language between the groups to better develop a common operating picture and coordinate response efforts within an ICS framework. The research also indicated a knowledge gap in practitioners with less than five years of experience, underscoring the need to include these practitioners in the cross training and exercise events.
- *Focus on the Common Operating Picture:* One of the biggest challenges identified in the research was the difficulty developing a common operating picture during a significant cyber event. Beyond training to increase the use of common terminology as mentioned above, pre-negotiation should occur between EM/HS and IT/CS leaders regarding platforms, protocols and participants required as part of a communications plan. Taking it one step further, the leaders should pre-negotiate as much as possible who will assess the technical cyber impacts and who will assess the second and third order effects. Training on a common terminology and pre-negotiating these tasks will help to more quickly develop a robust common operating picture that can be used to establish unified strategies, priorities and plans of action.

- *Integrate Communications & Pre-Plan for Multiple Response Locations:* Cyber incident responders should prepare for two or more response locations, a central command location and the location(s) where information technology infrastructure that may be impacted. The central command location, such as a State Emergency Operations Center (SEOC), could be used to coordinate response efforts with impacted locations and for second order effects. The on-site technical response location(s) should pre-plan logistics for an expanding response team. Both EM/HS and IT/CS responders would benefit from creating communications plans that include secondary and tertiary communications platforms as the primary response location is likely to have their communications systems impacted by the cyber event.
- *Implement Comprehensive IT/CS Human Resource Management:* There is a scarcity of technical IT/CS human resource response assets indicated by the research, resulting in the need for efficiency in the resource's management. To facilitate better resource management, IT/CS and EM/HS leaders should collaborate to create a comprehensive list of potential response assets while ensuring that the EM/HS leaders have a true understanding of each asset's capabilities. Additionally, the leadership team should continually evaluate assignments of response assets during an event to ensure that IT/CS technical experts are not tasked with non-technical tasks, thus freeing them to focus on their areas of expertise.

Implementing the Incident Command System is not a guarantee for success in a significant cyber incident response. History has shown many examples of disaster response failures when ICS was implemented, but the research has shown that its implementation during a cyber disaster can improve the response efforts. ICS is already the de facto standard for incident response for EM/HS and it is also identified by the National Cyber Incident Response Plan as the framework to be adopted.[7] Overall,

[7] Harrald, "Agility and Discipline," 263; U.S. Department of Homeland Security, *National Cyber Incident Response Plan* (Washington, DC: Department of Homeland Security, 2016), 8, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

while not perfect, ICS is a useful framework for connecting the technical cyber incident responders to the broader response community. This thesis can help further improve its implementation.

ACKNOWLEDGMENTS

First and always, thank you to my wife and daughter. Lynn, your support and unwavering belief in me are more than I deserve. I could not have completed this program without everything you took on so that I had time to study. Delaney, may you someday understand why Dad missed this time with you, and recognize the importance of always learning. I hope in the future you read this and think, “Not bad, but I can do it better.” No doubt, you can. To my parents, thank you for setting high expectations for me and always supporting me in my reach to meet them.

May I also be intentional with my gratitude to my co-workers at the ND Department of Emergency Services and the ND State & Local Intelligence Center. You all came through for me any time I needed someone to cover me, and I appreciate it. In particular, thank you Amy Anton, Cody Schulz, and MG Alan Dohrmann for allowing me to pursue this great opportunity. I promise to put this knowledge into practice to better serve the citizens of North Dakota.

To my advisors, Glen Woodbury and Lauren Fernandez, thank you! First, thank you for always being positive and moving me forward. Second, thank you for challenging me and making me do better. Your advice was always appreciated, even when I disagreed. Marc Pritchard, besides me, no one did more to help get this thesis across the finish line. You won’t show up in the official advisors listing, but without you my survey data would have been useless. Thank you for turning me into a fledgling quant.

I cannot forget to thank the entire staff at NPS/CHDS. There is no way to mention everyone who helped along the way, but there was never a need or question that wasn’t addressed quickly and with a smile. The instructors, GWC, DKL, and support staff took care of me and my classmates in a way I didn’t think was possible. It was a tough year as we transitioned to a virtual-only format, but you pulled it off. 1905/1906, I can honestly say I learned something from each of you. I’ll never forget thinking after the first IR how smart and talented you all were, and I was right. For each of you, I am grateful.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE INCIDENT COMMAND SYSTEM IN SIGNIFICANT CYBER INCIDENTS

A. PROBLEM STATEMENT

In February 2018, the Colorado Department of Transportation was hit with a ransomware attack of such brute force that it rendered the agency nearly inoperable and resulted in the first-ever state emergency declaration for a cyber incident.[1] That incident was followed by large-scale attacks on the municipalities of Atlanta and Baltimore as well as the state networks of Texas and Louisiana, among others.[2] In the 2019 "Worldwide Threat Assessment," the director of national intelligence stated that U.S. adversaries and competitors will increase their use of cyber capabilities "to steal information, to influence our citizens, or to disrupt critical infrastructure."[3] As society becomes more reliant on interconnected cyber systems in both government and critical infrastructure, the need for an effective government response to major cybersecurity incidents becomes more important. An ineffective response to these large-scale cyber incidents could have significant economic, national security, and even individual safety and health consequences for the people of the U.S.

Resulting from the 2003 Homeland Security Presidential Directive (HSPD)-5, the Department of Homeland Security issued National Incident Management System (NIMS) guidelines in 2004 and a follow-on edition in 2008.[4] Neither the 2004 nor 2008 edition

[1] Colorado Department of Transportation, *CDOT Cyber Incident*, 3.

[2] Herbert Dixon, "Cyberattacks on Courts and Other Government Institutions," *Judges' Journal* 57, no. 3 (Summer 2018): 37–39, ProQuest; Amelia A. Boylan, Audrey N. Tepe, and Danny W. Davis, "After the Ransomware Attacks: Texas Governance and Authorities for Cyberattack Response," Homeland Security Today, November 13, 2019, https://www.hstoday.us/subject-matter-areas/infrastructure-security/after-the-ransomware-attacks-texas-governance-and-authorities-for-cyberattack-response/; and State of Louisiana, "State of Emergency - Cybersecurity Incident" (Baton Rouge: State of Louisiana, July 24, 2019), https://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf.

[3] Coats, Worldwide Threat Assessment of the US Intelligence Community, 5.

[4] U.S. Department of Homeland Security, *National Incident Management System* (Washington, DC: Department of Homeland Security, 2008), https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

contained the word "cyber."[5] In the third edition, released in October 2017, the word "cyber" appears four times, which is on par with other terms such as flood, hurricane, or tornado.[6] As the template for managing incidents across the country, NIMS is relatively new to the management of cyber incidents. A key component of NIMS, the Incident Command System, is defined by FEMA as "a standardized approach to the command, control, and coordination of on-scene incident management."[7] Although there has been near-universal acceptance of NIMS and the Incident Command System (ICS) among government emergency response agencies due to statutory requirements, there are significant opportunities for adoption by private-sector and non-governmental organizations. With 85% of the nation's critical infrastructure held by private-sector partners based on a FEMA estimate, it becomes even more important to standardize a way for all agencies to interface in a worst-case scenario.[8] This need to interface was the reason NIMS and its critical component ICS were implemented in the first place after the September 11, 2001, terrorist attacks.[9]

Cyber attacks against the nation and its critical infrastructure are likely to increase in frequency, and these incidents will have ever-more serious consequences. Nevertheless, no extensive research exists on the effectiveness of ICS in significant cyber incidents, nor on how ICS may be used to improve cyber incident response. As new cyber response capabilities come online among different government agencies, the need to interface among them will become even more important. The central problem this thesis addresses is how ICS can be implemented to improve response in significant cyber incidents.

[5] U.S. Department of Homeland Security.

[6] Federal Emergency Management Agency, *National Incident Management System*, 3rd ed. (Washington, DC: Department of Homeland Security, 2017), https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

[7] Federal Emergency Management Agency, 24.

[8] Eileen R. Larence, Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics, GAO-07-39 (Washington, DC: Government Accountability Office, 2006), 1, https://www.gao.gov/assets/260/252603.pdf.

[9] Federal Emergency Management Agency, "NIMS and the Incident Command System" (Washington, DC: Federal Emergency Management Agency, November 23, 2004), https://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

B. RESEARCH QUESTION

Is ICS an applicable framework for responding to significant cyber incidents, and if so, how?

C. LITERATURE REVIEW

ICS has not been widely adopted or tested as a response framework for significant cyber events. While there has been substantial research on its effectiveness, there has yet to be rigorous research on the effectiveness of the system during cyber events. This literature review focuses on the development and history of ICS, purported strengths and weaknesses of ICS, and the use of response frameworks for significant cyber security incidents. An online search of Dudley Knox Library and Google Scholar provided relevant results dating as far back as 1978. The focus of this review is primarily on literature first published in 2001, the year that sparked a new age for emergency incident management.

1. History and Development of ICS

The development and goals of ICS shed light on its potential use in a significant cyber incident. NIMS was established in 2004 after the September 11, 2001, attacks on the World Trade Center.[10] One of its key components is ICS, which was established by the U.S. Department of Homeland Security (DHS) to be "a standardized approach to the command, control, and coordination of on-scene incident management that provides a common hierarchy within which personnel from multiple organizations can be effective."[11] ICS was originally developed in the 1970s by fire-fighters in California and had already been considered the de facto standard by emergency management and fire-fighting disciplines when the federal government added NIMS and ICS as a compliance measure for states to receive grant funding.[12] Burgiel identifies eight core concepts of ICS:

[10] Austen Givens, "Strengthening Cyber Incident Response Capabilities through Education and Training in the Incident Command System," *National Cybersecurity Institute Journal* 2, no. 3 (2015): 65, http://publications.excelsior.edu/publications/NCI_Journal/2-3/nci-journal-vol-2-no-3.pdf#page=67.

[11] Department of Homeland Security, *National Incident Management System*, 24.

[12] Erik Auf der Heide, *Disaster Response: Principles of Preparation and Coordination* (St. Louis, MO: Mosby, 1989), 134–35; and Harrald, "Agility and Discipline," 263.

"common terminology, integrated communications, modular organization, recognized command structure, manageable supervisory structure, consolidated action plans, comprehensive resource management, [and] pre-designated incident facilities."[13]

2. Benefits and Critiques of ICS

A review of the literature reveals an overarching divergence of appraisals between practitioners of ICS and academic researchers. Practitioners by and large praise ICS and its potential as a system for coordination during a crisis while academics question the system's ability to meet its stated goals.[14] There was no shortage of literature available for this review, which also included Incident Management Systems and NIMS when the discussion related to ICS. There was, however, a dearth of empirical or quantitative research available on the successes or failures of ICS. As pointed out by Jensen and Thompson, much of the research viewed as critiquing ICS was not based on new research and lacked empirical evidence while failing to address ICS specifically in favor of critiquing command-and-control models.[15]

Many of the proponents of ICS praise its flexibility and scalability as primary virtues.[16] Bennett describes ICS as "a modular, flexible, standardized system used by emergency responders to ensure efficient resource management resulting in a safe, efficient, effective response."[17] Although limited to one fire battalion, research conducted by Bigley and Roberts found three factors related to ICS reliability: structuring

[13] Stanley W. Burgiel, "The Incident Command System: A Framework for Rapid Response to Biological Invasion," *Biological Invasions* 22, no. 1 (2020): 158, https://doi.org/10.1007/s10530-019-02150-2; and "Overview of MSCC, Emergency Management and the Incident Command System," in *Medical Surge Capacity Handbook: A Management System for Integrating Medical and Health Resources During Large-Scale Emergencies*, 2nd ed. (Washington, DC: Department of Health and Human Services, 2007), https://www.phe.gov/Preparedness/planning/mscc/handbook/chapter1/Pages/emergencymanagement.aspx.

[14] Jessica Jensen and Steven Thompson, "The Incident Command System: A Literature Review," *Disasters* 40, no. 1 (January 2016): 160, https://doi.org/10.1111/disa.12135.

[15] Jensen and Thompson, 161.

[16] Perry, "Incident Management Systems in Disaster Management," 411; Christen et al., "An Overview of Incident Management Systems," 6; Bigley and Roberts, "The Incident Command System," 1283; and Bennett, "Effective Emergency Management," 31.

[17] Bennett, "Effective Emergency Management," 31.

mechanisms, constrained improvisation, and cognition management.[18] While many of the critiques of ICS include a lack of training and exercise as a key reason for poor ICS implementation, one academic review concludes that "in the United States clearly the best 'bang for the buck' lies with developing ICS-based emergency support systems that can be rapidly implemented under field conditions, and with the minimum of additional training."[19]

There are several evaluations of ICS following significant incidents. In researching the impact of its network structure, Moynihan reviewed several implementations of ICS, concluding that, overall, ICS works well in most cases but fails in the most serious circumstances.[20] Similarly, Buck, Trainor, and Aguirre conducted an evaluation of ICS by reviewing its application in nine disasters, concluding that ICS has broad applicability and is "more or less effective depending on specific characteristics of the incident and the organizations in which it is used."[21]

Even academics who support ICS recognize there are shortcomings that still need to be rectified. For example, Hannestad notes that "ICS may well not be the 'ideal' structure for large-scale emergency management, but at least in the United States it is currently 'the only game in town.'"[22] While practitioners have extolled the virtues of ICS, academic research has challenged its effectiveness in application and the ability to meet stated goals. While not critiquing NIMS as a system, Lester and Kreji discuss the need for transformational leadership to ensure that NIMS will be effectively implemented.[23] The

[18] Bigley and Roberts, "The Incident Command System," 1286.

[19] Stephen E. Hannestad, "Incident Command System: A Developing National Standard of Incident Management in the U.S.," in *Proceedings of the 2nd International ISCRAM Conference*, ed. B. Van de Walle and B. Carlé (Brussels: Information Systems for Crisis Response and Management, 2005), 26, http://idl.iscram.org/files/hannestad/2005/559_Hannestad2005.pdf.

[20] D. P. Moynihan, "The Network Governance of Crisis Response: Case Studies of Incident Command Systems," *Journal of Public Administration Research and Theory* 19, no. 4 (2009): 911, https://doi.org/10.1093/jopart/mun033.

[21] Buck, Trainor, and Aguirre, "A Critical Evaluation of the Incident Command System and NIMS."

[22] Hannestad, "Developing National Standard," 25.

[23] William Lester and Daniel Krejci, "Business 'Not' as Usual: The National Incident Management System, Federalism, and Leadership," *Public Administration Review* 67 (2007): 84–93, https://doi.org/10.1111/j.1540-6210.2007.00817.x.

focus on implementation is a recurring theme in academic works. Much of the existing empirical research on ICS centers on the implementation of NIMS, resulting in critiques of both organizational and structural failures to successful implementation. Interestingly, while these scholars have critiqued the implementation, most have refrained from critiques of NIMS as a structure or caveated their research as stating that the structure is not the problem.

A separate but closely related area of literature focuses on command and control as an organizational structure in disaster response. Most of this research was conducted by social scientists and did not include quantitative or empirical evidence. Wise concludes that command and control structures are not a good fit for emergency management/ homeland security (EM/HS) due to their hierarchal nature, which treats information as a "scarce resource" that is centralized at the top of organizations where decisions are made.[24] He goes on to say that adaptive management should be put in place, emphasizing an iterative process of learning during a disaster and collaboration amongst stakeholders, while simultaneously acknowledging that it is not meant to be "a substitute for functional management protocols" such as ICS.[25] In their 2006 review, Waugh and Strieb question practitioner claims of flexibility, focusing on leadership and collaboration during an incident as key factors for successful incident response.[26] They note, in reference to some recommendations for greater command and control during incident response, that "greater capacity for command and control is not synonymous with greater capacity for collaboration."[27]

[24] Charles R. Wise, "Organizing for Homeland Security after Katrina: Is Adaptive Management What's Missing?," *Public Administration Review* 66, no. 3 (2006): 310, https://doi.org/10.1111/j.1540-6210.2006.00587.x.

[25] Wise, 314.

[26] William L. Waugh and Gregory Streib, "Collaboration and Leadership for Effective Emergency Management," *Public Administration Review* 66 (2006): 131–40, https://doi.org/10.1111/j.1540-6210.2006.00673.x.

[27] Waugh and Streib, 137.

3. Response Frameworks in Significant Cyber Events

Due to the relative newness of cyber incidents with significant impacts, there has been little academic rigor applied to ICS in cyber incident response. In one of the most cited critiques of ICS, Wenger, Quarantelli, and Dynes—as quoted in Jensen and Thompson—conclude, "ICS does not appear to be a useful model that is readily transferable to broader communitywide planning and response efforts."[28] One of the key reasons they note is the difficulty integrating non-traditional responders into an ICS structure, which is a recurring theme of critiques of the system. This is particularly important in a cyber incident as the primary responders are likely to be technicians with information technology backgrounds. In her Naval Postgraduate School thesis, Emily Jane McLoughlin questions the effectiveness of ICS in an incident that involves cascading impacts to critical infrastructure, especially a cyber incident, due to the system's inability to incorporate second- and third-tier responders.[29]

Some applicable works reference ICS in a positive manner relative to cyber incidents, but much like other practitioners' efforts, there is no empirical evidence to support these conclusions. Givens recommends ICS as a structure to organize a cyber incident response, as well as for it to be incorporated into academic and professional cyber response training.[30] Givens also explores the lack of incident command training in collegiate cyber programs as well as the most common cyber certifications. Although his work references a biological invasion, Burgiel notes, "ICS application would facilitate cooperation among government agencies and their partners, improving the effectiveness and cost-efficiency of interventions."[31] At a minimum, this finding shows the potential for

[28] D. Wenger, E. Quarantelli, and R. Dynes "Is the Incident Command System a Plan for All Seasons and Emergency Situations?," *Hazard Monthly* 10 (March 1990), 12, quoted in Jessica Jensen and Steven Thompson, "The Incident Command System: A Literature Review," *Disasters* 40, no. 1 (January 2016): 161, https://doi.org/10.1111/disa.12135.

[29] Emily Jane McLoughlin, "Beyond the First 48: Incorporating Nontraditional Stakeholders into Incident Response" (master's thesis, Naval Postgraduate School, 2020), http://hdl.handle.net/10945/66108.

[30] Givens, "Strengthening Cyber Incident Response."

[31] Burgiel, "The Incident Command System," 163.

broader applicability of the system and may be closely associated with a cyber event, considering the similarities between computer and biological viruses.

4. Summary

ICS was initially developed by fire fighters as a way to standardize command, control and coordination during major wildfires. There are other frameworks that could be implemented during significant cyber incident response; however, the current de facto standard for disaster response is ICS and it is considered by some to be the "best bang for the buck" in the United States.[32] The system is also a measurement of performance for federal grant funding, further emphasizing its importance as a response framework. A combination of a federal requirement for ICS implementation for grant funding and a no-cost ICS training curriculum provided by FEMA are expected to have created a large pool of trained EM/HS personnel. These factors have led to the framework's application across virtually all types of disasters, yet it has not been frequently applied to significant cyber incidents.

In general, academics are not convinced of the framework's applicability due to a historical failure to meet its stated goals while practitioners by in large praise the system for coordination during crises. Proponents of the system praise its modularity, flexibility, and standardization while the system's opponents point to significant failures revealed in evaluations of its use during disasters. The research that does exist on ICS/NIMS is nearly all qualitative and tied more closely to command and control in general, rather than quantitative or empirical and closely aligned with ICS. This thesis aims to address the gaps in the research both in terms of the application of ICS in significant cyber incidents, but also in providing a quantitative element to the body of research.

[32] "Hannestad - 2005 - Incident Command System A Developing National Sta.Pdf," 26, accessed May 15, 2020, http://idl.iscram.org/files/hannestad/2005/559_Hannestad2005.pdf.

II. METHODOLOGY

This thesis uses a mixed method study consisting of three methods designed to identify and analyze strengths, weaknesses, and gaps in significant cyber incident response. The three methods include interviews, case studies, and surveys. The *National Cyber Incident Response Plan* provides a definition of "significant cyber incident" for use in the research: "A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[33] This study is centered on the eight core concepts of ICS, which were used as the primary framework for the coding of research data. The outcomes from each of the three methods are synthesized to examine if ICS could improve the response to a significant cyber incident. Finally, through the synthesis of these methods, this research provides recommendations for improving cyber incident response.

A. FRAMEWORK

The eight core concepts of ICS are central to this research and serve as the primary framework for categorizing qualitative findings and qualitative results. The U.S. Department of Health and Human Services provides the following definitions for each core concept in Exhibit 1–3. Incident Command System Core Concepts.[34]

- Common terminology - use of similar terms and definitions for resource descriptions, organizational functions, and incident facilities across disciplines

- Integrated communications - ability to send and receive information within an organization, as well as externally to other disciplines

[33] Department of Homeland Security, *National Cyber Incident Response Plan* (Washington, DC: Department of Homeland Security, 2016), 8, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[34] Department of Health and Human Services, "Overview of MSCC, Emergency Management and the Incident Command System."

- Modular organization - response resources are organized according to their responsibilities. Assets within each functional unit may be expanded or contracted based on the requirements of the event

- Unified command structure - multiple disciplines work through their designated managers to establish common objectives and strategies to prevent conflict or duplication of effort

- Manageable span of control - response organization is structured so that each supervisory level oversees an appropriate number of assets (varies based on size and complexity of the event) so it can maintain effective supervision

- Consolidated action plans - a single, formal documentation of incident goals, objectives, and strategies defined by unified incident command

- Comprehensive resource management - systems in place to describe, maintain, identify, request, and track resources

- Pre-designated incident facilities - assignment of locations where expected critical incident-related functions will occur

The provided definitions were used throughout this thesis. In addition, the definitions were adapted to create the question set (Appendix A) for the quantitative survey.

B. QUALITATIVE INTERVIEWS

Senior leaders in EM/HS and computer information technology/cybersecurity (IT/CS) were interviewed to gain depth of knowledge in strengths, weaknesses, expectations, and recommendations for cyber incident response. Throughout this study, the fields of EM/HS are combined, as are the IT/CS fields. The fields were combined based on an assumed close relationship and overlap of some duties depending on location and/or organization. Still, there are differences between emergency management and homeland security, as there are differences between information technology and cybersecurity that should be considered when contextualizing the data and outcomes of this study. EM/HS and IT/CS are both used broadly in the context of this research in order to simplify quantitative data analysis and categorize qualitative data. Interview findings were used to triangulate qualitative findings from the case studies and quantitative results. Prioritization for interviews was given to senior leaders who have experience in responding to significant cyber events. Whenever possible, if a key leader from one discipline was interviewed, his or her organizational counterpart was also interviewed. For example, when the state director of emergency management was interviewed, the state chief information security officer was also sought out for interview. The sample size for interviews consisted of eight respondents, representing five locations, and included four IT/CS professionals and four EM/HS professionals. It was desirable to interview multiple disciplines from the same jurisdiction to provide further context to the other's answers because they may relate to shared experiences from different perspectives. The objective of the personal interviews was to identify strengths, weaknesses, and gaps specific to incident response management. Interview questions were also included that specifically addressed the core concepts of ICS and NIMS. The full semi-structured interview question set is available in Appendix A. Table 1 lists all interview participants.

Table 1. Qualitative Senior Leader Interview Subjects

Name	Title	Organization	Interview Date
Andrew Phelps	Director	Oregon Office of Emergency Management	10/10/2020
Deborah Blyth	Chief Information Security Officer	Colorado Governor’s Office of Information Technology	10/13/2020
Kevin Ford	Chief Information Security Officer	North Dakota Information Technology Department	10/13/2020
Michael Willis	Director	Colorado Office of Emergency Management	10/16/2020
Cody Schulz	Director	North Dakota Homeland Security Division	10/16/2020
David Allen	Chief Information Security Officer	Georgia Technology Authority	10/27/2020
Mark Sexton	Deputy Director of Programs and Finance	Georgia Emergency Management and Homeland Security Agency	10/28/2020
Shane Swanson	Deputy Chief Information Security Officer	Texas Department of Information Resources	1/12/2021

Each semi-structured interview was conducted using a recorded video call. Participants were provided an interview guide when scheduling, providing information about the topics to be discussed, and to set interview expectations. Upon completion of the recorded call, interviews were transcribed using the intelligent verbatim transcription method. Interview data was coded first using a deductive method, where interview excerpts were assigned to each of the eight core concepts of ICS. Additionally, inductive coding was used to identify emergent themes by applying grounded theory.

Notably, overlap between interviews, case study incidents, and quantitative data analysis was expected. This was an intentional effort to create a deeper understanding of the case study findings and survey results, where the coded interview data is used. Due to the interconnected nature of the interviews and case studies, there was the potential for incidental identification of anonymous participants by the process of elimination. All senior leaders interviewed authorized attribution for the research. The Naval Postgraduate School Institutional Review Board approved the semi-structured interview protocols as NPS.2020.0059-IR-EP7-A.

C. CASE STUDIES

Two case studies are presented to provide a qualitative analysis of significant cyber incidents. The cases include the 2018 Colorado Department of Transportation (CDOT) Case and the 2019 Texas Municipality Case. Additional, relevant cases were excluded due to the lack of available information. Both case studies focus on a singular significant cyber incident using publicly available documents, interviews, and reports as well as documents obtained using open records requests when available. Individual incident case studies aim to provide generalizable conclusions about the application, or lack thereof, of an incident management system in a cyber event. Individual case studies are written in the emic perspective and consist of four parts:

- Introduction and Background: describes the incident in general, significant factors, and outcomes
- Analysis by Core Concept: assigns relevant information from the case to each core concept of ICS
- Emergent Themes: relates relevant emergent themes not attributed to the core concepts of ICS
- Summary: a brief summary of the case

The case studies conclude with a cross-case analysis that provides a brief comparison between the events, an in-depth analysis of the eight ICS core concepts as they relate to the cases, and emergent themes from the cases. Each core concept and emergent theme is analyzed by first summarizing the findings of the case materials and then second through an analysis of the relevant interview findings.

D. QUANTITATIVE SURVEY

The third method of analysis is an anonymous survey designed to identify the perceptions of incident management systems from both EM/HS and IT/CS professionals. Specifically, the survey will collect data on their perceptions of eight core concepts of ICS, as identified by Burgiel: "common terminology, integrated communications, modular organization, recognized command structure, manageable supervisory structure, consolidated action plans, comprehensive resource management, [and] pre-designated incident facilities."[35] Perceptions of internal and external organizational response capabilities are compared and contrasted, as is data across levels of career progression and field of discipline. There is an expectation that information technology practitioners will have vastly different perceptions of incident response from emergency management/ homeland security practitioners.

The survey consists of two primary sections. In the first section, non–personally identifiable demographic information was collected to establish the field of discipline, level in organizational structure, and years of experience in their field of discipline. Further questions were posed to determine the respondents' familiarity, experience with, and application of incident management systems. Efforts were taken to ensure that any demographic information collected cannot be used to identify individual participants. The purpose of this section was to provide context to the primary survey goal of identifying incident management perceptions.

The second section of the survey collected data on the respondents' perceptions of their organization's ability and external organizations' ability to respond to a significant cyber event. This portion of the survey used a seven-point Likert scale. In addition, each survey question for internal and external organizations consisted of a positive and negative indicator statement placed randomly in the survey for each core concept. Two sample questions are shown in Figure 1 to demonstrate the positive and negative indicator statements for a core concept.

[35] Burgiel, "The Incident Command System," 158; and Department of Health and Human Services, "Overview of MSCC, Emergency Management and the Incident Command System."

Sample Survey Questions						
My organization uses common terminology during incident response that is easily understood by outside agencies.						
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○
Common terminology that is easily understood by external organizations is not used by my organization.						
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

Figure 1. Sample Questions for Survey

The goal sample size of the survey was a minimum of 30 respondents per sample grouping of EM/HS or technical computer IT/CS professionals. In addition, a minimal goal of three per subgroup of practitioner level, mid-management level, or senior leadership was set. Recruitment for the survey took place across multiple online venues. A survey link was posted in common industry and professional forums, LinkedIn, and through direct emails to interview participants and relevant organizations. The survey opened on October 1, 2020 and was closed on January 13, 2021, having met the minimum stated goals from the IRB request. The survey was open for 105 days and received 84 total responses, of which, three participants did not consent to participate in the research and were excluded.

Microsoft Forms served as the online survey tool for this study. Participation in the study was voluntary and anonymous. The survey consisted of an informed consent question, nine demographic questions, and 32 questions about the participants' perceptions of response capability. The response capability questions were divided into 16 questions for perceptions of the participant's own organization and 16 questions regarding his or her perceptions of external agencies they interact with. The 16 questions referenced one of the eight core concepts of ICS, with a positive and negative indicator for each concept. One error occurred in the creation of the survey, resulting in only a single positive indicator question for the concept of "pre-designated facilities," while the concept of "Integrated Communications" had a positive indicator question and two negative indicator questions.

The error is not believed to have significant impact on the data. See Appendix B for the full question set.

A data validation and cleaning process was completed prior to analysis. The participants were sorted into the two primary categories of IT/CS and EM/HS. A review of the data set examined each submission for incomplete and erroneous entries as well as duplicate entries. As this study focused on the specific perspectives of IT/CS and EM/HS professionals, exclusion of responses from those outside of these fields (two submissions) improved the reliability of the subsequent analyses.

Data analysis utilized JMP Pro 15 and Microsoft Excel, focusing on descriptive statistics, means, comparisons, and the development of Pearson's correlation coefficients to provide an increased understanding of the relationships among the eight core concepts. Recoding of the Likert-scale responses to continuous numeric values within the software allowed for the calculation of descriptive and inferential statistics. In order to recode the Likert-scale questions, answers to positive indicator statements were assigned values ranging from 7 for Strongly Agree to 1 for Strongly Disagree. Answers to negative indicator statements were assigned values inversely, as shown in Table 2.

Table 2. Numeric Likert-scale Values

Response	Positive Indicator Statement	Negative Indicator Statement	Mean Score Value (*M*)
Strongly Agree	7	1	7
Agree	6	2	6
Somewhat Agree	5	3	5
Neither Agree / Nor Disagree	4	4	4
Somewhat Disagree	3	5	3
Disagree	2	6	2
Strongly Disagree	1	7	1

A mean (*M*) value was calculated for each core concept based on the positive and negative indicator statements. The pre-designated Facility concept only had one question, thus no mean was calculated. This completed the conversion of the core concept Likert-scale data, resulting in a single average numeric value of survey participants' perceptions of their organizations' response to cyber activities. The newly calculated *M* values align with the response values assigned to the positive indicator questions shown in Table 2.

Four demographic subgroups were simplified by consolidating the categories within. The participants' length of experience in field (Experience) category was consolidated into two categories for analysis: less than 5 years (<5) and 5 or more years (≥5). The consolidation of the experience categories was based on an assumption that those with five or more years of experience were more likely to be familiar with frameworks and organizational plans. Further reasoning for the consolidation was the assumption that those with five or more years in the field would not gain significant knowledge on the frameworks or plans compared to their lesser experienced counterparts. The Organization subgroup was consolidated into four categories, Government (GO), Private Sector (PS), and Other (OT). The third demographic subgroup modification, prior incident response experience (Incident), was consolidated to the two categories of no response experience (NR) and experience with at least one cyber incident response (YR) in a significant cyber incident. A subgroup of responses for organization response plans combined into four categories to simplify analysis and improve reliability. The simplification and consolidation of the subgroups resulted in easier to understand results and larger sample pools.

The survey protocols have been approved by the Naval Postgraduate School's Institutional Review Board as NPS.2020.0058-IR-EM2-A.

E. LIMITATIONS

There were several limitations to the research methods. First, the restrictions on case study information available for review limited the depth of research that would otherwise be desirable. Further, not all senior leaders with substantial experience from the cases reviewed were available for interviews. The available information for case studies also was limited in scope to state-level, government response efforts, leaving out the private sector critical infrastructure partners.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES

A. METHOD

Two case studies were completed to provide a qualitative analysis of the response to the first and third cyber incidents resulting in state emergency declarations. The cases were selected to provide insight into what were assumed to be significant response efforts requiring multi-agency coordination and the application of NIMS/ICS due to the use of an emergency declaration. Efforts were made to analyze internal documents, academic papers, conference presentations, personal interviews, and open-source reporting as available. Source materials were then deductively coded to the eight core concepts of the Incident Command System as defined by Burgiel.[36] Then, relevant themes that were not attributable to any of the core concepts were identified. Finally, the findings from the eight qualitative senior leader interviews were applied to the case study findings.

B. CDOT RANSOMWARE CASE STUDY

1. Introduction and Background

The first case study for examination is centered on the Colorado Department of Transportation's (CDOT) ransomware attack of 2018. The review for this analysis consisted of the officially released after action report, one academic case study, two recorded presentations, two personal interviews, and publicly available news articles. Other internal documentation from the Colorado Department of Emergency Management and the Colorado National Guard was reviewed, documentation which provided insight into actual operations; however, it does not further the discussion of command and control in the event. One of the most important aspects of the CDOT case is that it provides an opportunity for a before and after analysis of ICS implementation. During the initial 10 days of response, ICS was not implemented, after which a Unified Command was established using ICS principles.

[36] Burgiel, "The Incident Command System," 158; and Department of Health and Human Services, "Overview of MSCC, Emergency Management and the Incident Command System."

The CDOT first became aware of a ransomware attack on Wednesday, February 21 of 2018, but it had likely been inactively waiting there since February 18th.[37] The attack infected approximately 150 servers and 2000 workstations within the agency and resulted in an initial response team coordinated by CDOT and the Colorado Governor's Office of Information Technology (OIT).[38] By February 28th, response team members believed they had the malware contained and began bringing systems back online; only to find their systems becoming reinfected with the malware.[39] It was at this time that the CISO for the state coordinated with the State Emergency Operations Center (SEOC) to gain more resources for the response efforts.[40] Simultaneously, the Governor issued a verbal emergency declaration which opened access to funding and the Colorado National Guard's assistance.[41] On March 1, Governor John Hickenlooper formally issued what would become the first statewide emergency declaration for a cyberattack.[42] This led to a deployment of National Guard assets to the CDOT headquarters and then the creation of a Unified Command on March 3.[43] Response efforts were carried out over the next several days until recovery operations officially began on Friday, March 10, when CDOT and OIT assumed combined command of the recovery phase that would last for weeks.[44] On March 14th, Unified Command was disestablished after coordinating a response that included 12 government organizations as well as numerous private sector cybersecurity contractors.[45] The ransomware attack resulted in costs of up to $2 million for the state.[46] The attacks

[37] Colorado Department of Transportation, *CDOT Cyber Incident*, 3.

[38] Colorado Department of Transportation, 3.

[39] Colorado Department of Transportation, 3.

[40] Colorado Department of Transportation, 3.

[41] Colorado Department of Transportation, 3.

[42] Benjamin Freed, "What Colorado Learned from Treating a Cyberattack Like a Disaster," StateScoop, May 15, 2019, https://statescoop.com/what-colorado-learned-from-treating-a-cyberattack-like-a-disaster/.

[43] Colorado Department of Transportation, *CDOT Cyber Incident*, 3.

[44] Colorado Department of Transportation, 3.

[45] Colorado Department of Transportation, 2.

[46] Benjamin Freed, "Indictments in Ransomware Spree on Cities, Agencies," StateScoop, November 28, 2018, https://statescoop.com/ransomware-spree-against-atlanta-newark-and-others-leads-to-indictment-of-2-iranians/.

were later to be included in an indictment against two Iranians who are accused of causing over $30 million in damages to several government and non-government organizations.[47]

2. Analysis by Core Concept

a. Common Terminology

As one of the core concepts of the Incident Command System, common terminology may be described in this context as two or more groups using the language that has a shared meaning among the groups. The CDOT ransomware attack did reveal challenges understanding the meaning of certain terms as well as the use of acronyms that had different meanings depending on area of expertise. One example of such an instance was discussed by Mike Willis, Colorado's Director of Emergency Management, during a presentation to the North Dakota Emergency Management Association. He discussed the use of ICS and TCP, which mean Incident Command System and Traffic Control Point to emergency management professionals while information technology personnel commonly refer to them as Industrial Control System and Transmission Control Protocol.[48] Similarly, the CISO for OIT Deborah Blyth has pointed out the need to translate between her organization and the Unified Command Group during the CDOT response when referring to terms such as a JIC (Joint Information Center) and Documentation Unit.[49] In a personal interview, Director Willis pointed out that "there is still a cultural and communication gap between cyber and other responders."[50] After her experience with the CDOT ransomware attack, CISO Blyth now is implementing NIMS into cyber response plans at her agency so that her team and other responders will be "speaking the same language."[51] She also has

[47] "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Justice News, November 28, 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[48] ″Michael Willis," August 29, 2019, ND Dept of Emergency Management IT Department, video, 1:06:56, https://www.youtube.com/watch?v=7gkDAHqO-24&feature=youtu.be.

[49] "Key Takeaways from the 2018 Ransomware Attack on Colorado DOT," October 10, 2019, Bismark State College, College Relations, video, 1:18:28, https://vimeo.com/369910099.

[50] Michael Willis, personal interview by author, Microsoft Teams Video Meeting, October 16, 2020.

[51] Deborah Blyth, personal interview by author, Microsoft Teams Video Meeting, October 13, 2020

remarked that emergency management Incident Management Teams (IMTs) asked to receive cyber-related training to better understand the cyber response team's needs.[52] She did acknowledge, though, that even without the training the IMTs could wrap the Incident Command System framework around a response and be successful.[53] Both Director Willis and CISO Blyth have indicated that there were challenges attributable to unfamiliarity with terminology across disciplines, however they were able to work through the issues even without the technical cyber responders having training on the incident command system. Based on the OIT's ongoing implementation of NIMS to enable the organization to "speak the same language," it indicates there is an acknowledged value to common terminology in a cyber response.

b. Integrated Communications

Integrated communications as a core concept did not appear frequently in the case study of the CDOT event. When asked directly if integrated communications were an issue in the CDOT incident, Director Willis stated that they were "not a thing" during the response.[54] This was attributed to the normal communication channel of computer network and voice over internet protocol (VOIP) phones being disabled during the cyber attack. He went on to state that during the response they were able to have all the responders co-located so they could communicate directly. Further communication was successfully established by using butcher paper on the walls and white boards in the command center.[55] As the incident progressed, the response team was able to use wi-fi hotspots to communicate with the State Emergency Operations Center for integration into their incident management platform and eventually requested and received a FEMA emergency communications resource to establish a computer network capability.[56] Although both

[52] Blyth.

[53] Blyth.

[54] Willis, personal interview by author.

[55] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack,"; and "Michael Willis."

[56] ND Dept of Emergency Management IT Department, "Michael Willis,"; and Willis, Personal Interview by Author

CISO Blyth and Director Willis acknowledged the importance of using the white boards and butcher paper to share priorities, it is unclear whether integrated communications played a significant role in this response.

c. Modular Organization

A third core concept of ICS is modular organization. There is a clear indication that implementing ICS in this event led to a positive outcome relative to the incorporation of numerous resources. Listed as a major strength in the after action review, after struggling for several days prior to employing ICS, the Unified Command Group was able to organize resources from five state agencies, six federal partners, and four private cyber security contractors in less than a week.[57] The After Action Report (AAR) also clearly identified the value in the recommendations section in the following statement: "This annex should address escalading [sic] cyber incidents, establish triggers for response actions, including establishing scalable command and control and assigning roles and responsibilities."[58] There were less clear indications that the concept of a modular organization is applicable to cyber incidents as well. One instance is when Director Willis discussed the difficulty of defining and assigning different teams to determine "exactly who does what."[59] An additional reference made was the description of the response organizational chart showing multiple agencies and how each group interacted with each other, which in the context of the references seemed to indicate the need to bring in different participants to fill roles.[60] In a personal interview with Director Willis, he summed up the need for modularity by referencing the "Team of Teams" concept described in General Stanley McCrystal's book and stated that the concept is used for other incidents but "we haven't gotten there with cyber."[61] Overall, it was clear that organizational modularity was an important component of a successful incident response to the key leaders of the CDOT responding agencies.

[57] Colorado Department of Transportation, *CDOT Cyber Incident*, 6.

[58] Colorado Department of Transportation, 8.

[59] ND Dept of Emergency Management IT Department, "Michael Willis."

[60] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack on Colorado DOT,"; and ND Dept of Emergency Management IT Department, "Michael Willis."

[61] Willis, Personal Interview by Author.

d. Recognized Command Structure

Another core concept that was discussed numerous times after the CDOT incident was the recognized command structure concept. Explicitly stated in the after action review as a recommendation, the state noted that the State Emergency Operations Plan (SEOP) Cyber Incident Annex should be revised to "address escalading [sic] cyber incidents, establish triggers for response actions, including establishing scalable command and control and assigning roles and responsibilities."[62] Colorado's Director of Homeland Security and Emergency Management during the incident, Kevin Klein, is reported as stating, "Somebody's got to be in charge, and that's where the incident command structure comes into place."[63] These comments are further impactful when combined with the notations in the "Opportunity for Improvement" section of the AAR. The AAR stated if the cyber incident response team would have had ICS trained personnel it could have led to a "common approach to incident handling and may have reduced friction points between the response team and the CDOT Continuity of Operations Plan (COOP) team."[64] One academic paper, focused on the use of exercises in cyber incident response between OIT and the Colorado National Guard prior to the CDOT incident, had previously identified the challenges the organizations would face navigating various factors, one of which was chains of command in incident response.[65] When asked about previous exercises during a personal interview with Director Willis, he described not including NIMS/ICS in the exercises as a mistake that had to be overcome with trust during the CDOT incident while referencing back to a previous statement about how CISO Blyth trusted him to organize the formal command and control.[66] The concept of recognized command structure appeared several times across sources, with the related challenges of establishing priorities

[62] Colorado Department of Transportation, *CDOT Cyber Incident*, 8.

[63] Freed, "What Colorado Learned from Treating a Cyberattack Like a Disaster."

[64] Colorado Department of Transportation, *CDOT Cyber Incident*, 1.

[65] Erik L. Moore et al., "Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation," in *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* (2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Oxford, UK: IEEE, 2019), 2, https://doi.org/10.1109/CyberSA.2019.8899736.

[66] Willis, personal interview by author.

for response, assigning roles and responsibilities, and friction amongst response organizations.

e. Manageable Supervisory Structure

Ensuring a manageable span of control did not appear to be a significant factor in the CDOT response efforts. One recurring comment was the difficulty "keeping people in their lane."[67] Along the same line, Director Willis noted during a lessons learned presentation the importance of defining "exactly who does what" on a cyber incident response team.[68] Conversely, when asked directly during a personal interview whether span of control was an issue during the incident he said that it was a non-factor as it had already been established before the ICS structure was implemented.[69] During the same interview he said the only instance he could think of was that CISO Blyth was probably exceeding her span of control initially by taking on too many roles herself. While not necessarily an indicator of the importance of a manageable span of control, in her personal interview with the author CISO Blyth described the value emergency management provided when geographically structuring response elements so that leadership knew where to find each element as well as for the responders to know where leadership was located when needed.[70] She also said in the interview that emergency management implemented a badging system that made tracking response personnel easier, which could have impacted the perceptions on the concept of a manageable span of control. There does not appear to be significant support that providing a manageable span of control in a cyber incident was a need during the CDOT response.

f. Consolidated Action Plans

Likely the most referenced topic by the senior leadership during the CDOT response was planning priorities, which are related directly to the core concept of

[67] ND Dept of Emergency Management IT Department, "Michael Willis."; and Blyth, personal interview by author.

[68] ND Dept of Emergency Management IT Department.

[69] Willis, personal interview by author.

[70] Blyth, personal interview by author.

consolidated action plans. In the conclusion of the AAR, the creation of the Unified Command Group (UCG) is credited with providing direction and a command and control structure to the response efforts which in turn "unified and focused the efforts of the numerous government and private contractors involved."[71] This was important, as there are references in multiple presentations and in the AAR as to how the response was team was not functioning well until after the creation of the UCG was implemented.[72] The UCG was able to sort out the multiple priorities across different organizations including the business operations of the CDOT as well the cyber response personnel.[73] In fact during a joint presentation with CISO Blyth, Director Willis stated: "The first thing we did was set a unified set of priorities."[74] Blyth credits this with allowing them to not only prioritize tasks, but also to ensure they get completed or "closed out," as she put it.[75] The way this was accomplished was through the setting of priorities through consensus, with the emergency management professionals essentially acting as "referees."[76] Part of the implementation for consolidated action plans was the continuous briefings on the status of actions in the daily morning briefs, further ensuring that responders stayed in their lanes and that tasks were completed. It is clear after reviewing the available information on the case that consolidated action plans played a significant, positive role in the CDOT response.

g. Comprehensive Resource Management

The concept of comprehensive resource management appeared in the reviewed case study materials to be closely aligned with consolidated action plans due to an apparent tie between prioritization and resource assignment. Listed as a major strength in the AAR, the

[71] Colorado Department of Transportation, *CDOT Cyber Incident*, 8.

[72] Colorado Department of Transportation, *CDOT Cyber Incident: After-Action Report*; ND Dept of Emergency Management IT Department, "Michael Willis"; and Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack."

[73] ND Dept of Emergency Management IT Department, "Michael Willis."

[74] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack."

[75] Blyth, personal interview by author.

[76] Freed, "What Colorado Learned from Treating a Cyberattack Like a Disaster."

use of the UCG and emergency management allowed the CDOT to focus on executing its COOP while OIT was freed up to focus on the cyber response.[77] One example of the value of resource management was when, prior to the formation of the UCG and the implementation of an ICS structure, the CISO and other key leaders were ordering pizza for every meal.[78] Other logistics issues that arose during the CDOT incident were problems with tracking who was working and on site, how much food to order, uncleaned restrooms, and insufficient manpower.[79] The UCG was eventually able to facilitate an Emergency Management Assistance Compact (EMAC) request for additional technical experts, however it was noted that they should have requested mutual aid sooner to provide relief for worn out employees.[80] The Unified Command Group also was able to get resources (MERS team & Hunt Identification and Response Team) from FEMA even without a Stafford Act Disaster Declaration.[81] Director Willis did recognize, though, that the same mutual aid systems used in other incidents are not yet developed for cyber incidents.[82] The management of resources, along with coordinated action plans to set the prioritization of resources, was a key topic and driver of operational success for the incident response.

h. Pre-designated Facilities

Of the eight ICS core concepts reviewed in this case, pre-designated facilities are one of the least discussed in the available materials. In fact, the concept did not show up at all in the written materials or in public presentations. When asked about the value of pre-designated facilities during a personal interview, Director Willis stated their use was

[77] Colorado Department of Transportation, *CDOT Cyber Incident*, 7.

[78] ND Dept of Emergency Management IT Department, “Michael Willis.”

[79] ND Dept of Emergency Management IT Department, “Michael Willis,”; Bismarck State College, College Relations, “Key Takeaways from the 2018 Ransomware Attack,”; and Freed, “What Colorado Learned from Treating a Cyberattack Like a Disaster.”

[80] ND Dept of Emergency Management IT Department, “Michael Willis.”; Freed, “What Colorado Learned from Treating a Cyberattack Like a Disaster.”; Bismarck State College, College Relations, “Key Takeaways from the 2018 Ransomware Attack.”; and Blyth, personal interview by author.

[81] ND Dept of Emergency Management IT Department, “Michael Willis.”

[82] Willis, personal interview by author.

helpful and he would encourage them.[83] He specifically mentioned the SEOC for handling logistics, the JIC for providing a unified public message, and the value of having the Department Operations Center (DOC) at the CDOT for a response headquarters. Specifically, at the DOC, the responders were able to communicate directly person-to-person by walking from table to table when needed.[84] Conversely, there was a reference to CDOT employees implementing their agency's COOP by taking their laptops to an alternate location. This could have been disastrous because the laptops would have connected remotely to the network and thus been infected.[85] As one CDOT employee put it, their COOP was better suited for a meteor hit than a cyber attack referencing how they were prepared to go off site and begin a response but that was not an option in their cyber attack.[86] The CDOT response shows that there was some value in having pre-designated facilities as part of their response; however, there is some conflicting information specific to cyber incidents that should be considered.

3. Emergent Themes

There were other key takeaways from the CDOT attacks that should be considered when evaluating incident response. One of the first and most important challenges in the response efforts was the initial assessment of both the cyber issues and the business issues.[87] This was expanded upon to more specifically include information sharing and incident assessment. Another key takeaway from the response was the need for emergency managers to acknowledge that they are responsible for cyber incident response, and to stop treating it like a "cyber thingy."[88] In order for emergency managers to better respond to these incidents, leaders from the response team recommend that emergency managers normalize cyber response by treating them the same way they do other incidents and focus

[83] Willis, personal interview by author.

[84] Blyth, personal interview by author.

[85] ND Dept of Emergency Management IT Department, "Michael Willis."

[86] ND Dept of Emergency Management IT Department.

[87] ND Dept of Emergency Management IT Department.

[88] ND Dept of Emergency Management IT Department.

on consequence management.[89] One last theme that reappeared was the need for different agencies to work together on exercises and planning before the incident, as well as to work better with other stakeholders on communications to include lessons learned after an event.[90] These underlying themes appeared across nearly all of the reviewed materials, while often not being explicitly stated.

4. Summary

The CDOT ransomware attack resulted in many cyber-firsts in the nation. As Willis and Blyth pointed out in a presentation on the incident, pertaining to a cyber incident it was the "first declaration of a state disaster; first use of a unified command group; first emergency mobilization of National Guard cyber capability; first emergency response by federal cyber partners and first use of EMAC for cyber incident response."[91]

C. TEXAS MUNICIPALITIES RANSOMWARE CASE STUDY

1. Introduction and Background

When Governor Greg Abbott of Texas signed Senate Bill 64 into law in June of 2019, he likely had no idea how soon it would be needed. The bill not only added "cybersecurity event" as a legally recognized disaster, but also authorized the state's National Guard to assist the Texas State Guard "with defending the state's cyber operations."[92] On August 16th of that same year, 23 municipalities within Texas were hit with the Sodinokibi ransomware as well as hidden remote access malware.[93] The impacted organizations included a water treatment plant and a law enforcement agency, as well as

[89] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attac*k.*"; and ND Dept of Emergency Management IT Department, "Michael Willis."

[90] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack.*"*; ND Dept of Emergency Management IT Department, "Michael Willis.*";* Willis, personal interview by author; and Blyth, personal interview by author.

[91] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack.*"*

[92] Relating to Cybersecurity for Information Resources, Texas S.B. 64, 86th Legislature, (June 07, 2019), https://legiscan.com/TX/text/SB64/id/2027269.

[93] Boylan, Tepe, and Davis, "After the Ransomware Attacks"; and "Texas Cybersecurity Update," April 28, 2020, TDEM TV, video, 23:58, https://www.youtube.com/watch?v=N9jhrrvf7zM.

several other government functions.[94] Within hours of the cyber attack's beginning the governor had declared an emergency, becoming only the third state in the country to do so.[95] Ultimately, the attack resulted in an eight-day response consisting of at least five state agencies, private vendors, the FBI, Department of Homeland Security, and other state and federal partners.[96]

A review of two redacted internal documents, four publicly available articles, and a recorded video related to the cyber attack has provided several direct and indirect lessons learned in relation to the eight core concepts of ICS. The response efforts did include the implementation of ICS at the state emergency management agency; however, it was not broadly applied across all response entities. Other response frameworks used were conventional military command and control as well as the National Institute of Standards and Technology (NIST) cybersecurity framework. It is acknowledged that a lack of internal documentation from many of the involved responding agencies and significantly any impacted agencies limits insight into the effectiveness of the response efforts.

2. Analysis by Core Concept

a. Common Terminology

One of the core concepts of the Incident Command System is the use of common terminology. Across all reviewed sources, there was no direct reference to any difficulty understanding terminology across agencies. In the Department of Information Resources' (DIR) internal "August incident hotwash #1 outcomes" document, there is a recommendation for all team members to complete recommended Texas Department of Emergency Management (TDEM) recommended training.[97] TDEM generally

[94] Benjamin Freed, "How Texas Used Its Disaster Playbook after a Huge Ransomware Attack," StateScoop, October 15, 2019, https://statescoop.com/texas-ransomware-emergency-declaration-nascio-19/; and TDEM TV "Texas Cybersecurity Update."

[95] Freed, "How Texas Used Its Disaster Playbook after a Huge Ransomware Attack."

[96] Texas Department of Information Resources, "Ransomware and Incident Response in Texas" (Austin, TX: Office of the Chief Information Officer, Texas Department of Information Resources, January 2020), 2.

[97] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes" (Austin, TX: Texas Department of Information Resources, n.d.), 1, accessed March 20, 2020.

recommends basic NIMS/ICS courses such as IS-100, IS-200, IS-700, and IS-800.[98] In addition, grant funded positions are required to complete the FEMA Professional Development Series of foundational courses for emergency management professionals.[99] The SOC 101 course identified specifically in the hotwash is a state-developed course that teaches the basics of the State Operations Center, key roles in the Emergency Management agency, and the WebEOC incident management system.[100] One may infer from this hotwash recommendation and the recommended TDEM trainings that common terminology would benefit cyber incident response. Conversely, the lack of specific references to common terminology across all sources may indicate its lack of applicability in cyber incidents or that common terminology is already being used. No clear desirability or undesirability was identified in the reference materials for the core concept of common terminology.

b. Integrated Communications

Closely related to common terminology is the core concept of integrated communications. There were numerous references in the case study materials to integrated communications as a method for improving response. In a presentation to the National Association of State Chief Information Security Officers (NASCIO), the Texas Chief Information Security Officer Nancy Rainosek stated that partnering with the TDEM allowed for the use of a unified secure chat app for real time updates as well as the WebEOC platform for organizing workflows.[101] The DIR's hotwash also noted that in order to improve communication, all likely DIR incident response members should pre-establish accounts with TDEM.[102] The DIR also referenced the use of TDEM for communication through the SOC and district coordinators using a redacted tool, noting this

[98] Paul Hahn, email message to author, January 28, 2021.

[99] Hahn; and Emergency Management Institute, "Professional Development Series (PDS) Courses," Independent Study Program (IS), accessed January 28, 2021, https://training.fema.gov/is/searchis.aspx?search=PDS.

[100] Hahn, email message to author.

[101] Freed, "How Texas Used Its Disaster Playbook after a Huge Ransomware Attack."

[102] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes," 1.

was a key driver to their success.[103] A challenge to integrated communications was identified in multiple sources, but specifically in the hotwash, noting that a communications tool needed to be adopted but that not everyone needed access to some information.[104] The hotwash further recommended a tiered model of access to the information, such as the military PACE planning which consists of primary, alternate, contingency, and emergency communications methods. The multiple references to communications methods among groups may be interpreted as a key factor for successful incident response.

c. Modular Organization

There were limited references to modular organization across the identified sources; however, the references found do indicate an acknowledgment of the need for scalability, while also indicating that there was not a problem during this incident. In the DIR's June 2020 Incident Response Team Redbook, there are several references to the need for integration of ad hoc team members and subject matter experts.[105] In a case study of the incident, an intrastate cybersecurity mutual aid system has also been recommended, indicating further potential applicability for modularity in cyber incident response.[106] Prior to the incident, the Texas Military Department (TMD) had previously been used modularly in operations as part of the State of Texas Cyber Incident Response Team.[107] The accumulation of these indirect references shows that there was already likely an assumption for the need for scalability; however, it does not appear to be clearly codified in cyber incident response documents.

[103] Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3.

[104] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes," 1.

[105] Texas Department of Information Resources, *Incident Response Team Redbook* (Austin, TX: Texas Department of Information Resources, 2020), 24–26, https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template.pdf.

[106] Boylan, Tepe, and Davis, "After the Ransomware Attacks."

[107] Boylan, Tepe, and Davis.

d. Recognized Command Structure

Across all reviewed sources, there was minimal reference to any difficulty recognizing or understanding the command structure. The DIR did list "that there is no central designated agency for local entities to report incidents to…" as a lesson learned from the incident, indicating a lack of known command structure.[108] An inverted concern of the command structure was noted in the hotwash, noting that response resources won't know who the point of contact in the field is beforehand.[109] This may show the need for a known command structure for authentication of responders. As was noted previously, the hotwash recommendation for the cyber response team to complete any recommended TDEM training could also be viewed as indirect support for Unified Command or other ICS based command structure. Though there is no clear stated need for more clearly identifying the command structure, the references to a lack of a central reporting agency, the need for verification and authentication of response personnel, and the recommendation to complete TDEM training seems to acknowledge the need for an identifiable chain of command.

e. Manageable Supervisory Structure

The core concept of maintaining a manageable supervisory structure was not easily identified as a need or challenge in the source material reviewed. There was only one notable reference that applied to this concept. In the hotwash document, one of the issues described was that process and team composition throughout an incident should follow the regional model.[110] The hotwash also referenced desirability of pre-distributed resources for "faster first contact across the massive geography." This appears to indicate an appropriate division of resources, including human responders, would be able to serve better by organizing the teams. However, the same bullet point also discusses a tiered model for communication and incorporating other stakeholders for information sharing.[111]

[108] Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3.

[109] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes."

[110] Texas Department of Information Resources.

[111] Texas Department of Information Resources.

Due to the uncertainty, again, a clear indication of the need to better manage human resources was not able to be identified.

f. Consolidated Action Plans

In contrast to previous core concepts, the concept of consolidated action plans had multiple indications in the study. One of the most significant indicators of the need for consolidated action plans was the inclusion of templates for meeting minutes and updates that list actions to take and the next scheduled meeting.[112] The documents mirror key concepts in emergency management planning such as a scheduled battle rhythm, goal and objective development, and implementation of incident action plans. The need for focused action plans also was stated in the hotwash as a need to formulate reporting requirements to allow focus on response activities.[113] The desire for a coordinated plan had already been established prior to the incident in 2017 Texas House Bill 8, which required DIR to create a statewide incident response plan, and was noted as a key preparation measure.[114] Further evidence of the need for consolidated action plans were the mention of triage and prioritization in the hotwash and incident response report.[115] The reporting of the collaboration on response as both key in preparation and as a lesson learned show the applicability of this core concept to significant cyber incidents.

g. Comprehensive Resource Management

"Another benefit about working with TDEM is that they fed us, oh my gosh," was a quote from Texas CISO Nancy Rainosek when presenting at the National Association of State CISOs; emphasizing a shared experience with Colorado's success in resource management during the CDOT incident.[116] The core concept of comprehensive resource management was closely related to the information on consolidated action plans. In order

[112] Texas Department of Information Resources, *Incident Response Team Redbook*, 27–28.

[113] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes."

[114] Texas Department of Information Resources, "Ransomware and Incident Response in Texas."

[115] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes"; and Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3.

[116] Freed, "How Texas Used Its Disaster Playbook after a Huge Ransomware Attack."

to prioritize resource usage, as referenced in the ransomware report as a lesson learned, comprehensive resource management is implied.[117] A probable connection between the two would be that actions taking place are taken by responders, who are themselves resources. More significantly, the DIR's hotwash identified the need for a method in which the remote responders could be made aware of available resources.[118] Additionally, a previous case study identified the current and future use of emergency declarations under the Stafford Act as a way to, as it stated, "ensure that Texas has the resources to fully recover after a cyber incident."[119] In order to recoup these resources, though, proper documentation and accounting of eligible resources must occur. There was further documentation regarding compiling the costs of the incidents in the DIR's response redbook.[120] With the explicit documenting of the need for triage and prioritization, the potential for reimbursement under the Stafford Act, and recognition by the state CISO, comprehensive resource management as a desirable core concept has been established.

h. Pre-designated Facilities

The last of the core concepts to be explored in this incident is the establishment of pre-designated facilities. The first lesson learned listed in the public report by DIR is the use of the TDEM SOC as a key to the response success.[121] Pre-designation of facilities was also indicated in the hotwash when it stated, "Establish multi-hazard event location for the cyber team. This may be another room within the SOC or perhaps the NSOC. The location should be identified and known."[122] NSOC, as referred to in the previous quote indicates a Network Security Operations Center. This is a clear and explicit acknowledgment of the desirability for pre-designated facilities for incident response.

[117] Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3.

[118] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes."

[119] Boylan, Tepe, and Davis, "After the Ransomware Attacks."

[120] Texas Department of Information Resources, *Incident Response Team Redbook,* 21.

[121] Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3.

[122] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes."

3. Emergent Themes

Although not clearly aligned with any core concepts, there were two recurring themes amongst the response documents. One was the state's commitment to continuous improvement through after-action meetings and reports.[123] The second was a difficulty identifying and sharing the right information with the right partners during an incident due to ongoing criminal investigations of the cyber incident during the response.[124] These two challenges may require additional research to identify best practices.

4. Summary

In summary, the Texas ransomware event on August 16, 2019 clearly identified several core concepts as desirable while also leaving some concepts unindicated. There was a clear applicability and desirability for integrated communications, consolidated action plans, comprehensive resource management, and pre-designated incident facilities. There was much less certainty around the need to adopt common terminology, modular organization, recognized command structure, and manageable supervisory structure. The overarching theme of cyber incident response in Texas may best be described using a quote from the former Texas DIR Deputy CISO Andy Bennett: "I see the future of Texas security, cybersecurity, information security as collaborative. It is a team sport, and it is a full contact team sport."[125]

D. CROSS-CASE ANALYSIS

The review of the case materials provided indications that some of the eight core concepts were either more important in a significant cyber incident or were more problematic. In addition, there were three important topics that emerged in the review. This section includes the summary of these findings along with further supporting findings from the qualitative senior leader interviews.

[123] Texas Department of Information Resources, *Incident Response Team Redbook*, 37–40, 21, 23.

[124] Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes"; Texas Department of Information Resources, "Ransomware and Incident Response in Texas," 3; *Texas Cybersecurity Update*.

[125] TDEM TV, "Texas Cybersecurity Update."

1. Comparison of Incidents

There were several similarities between the CDOT and TX municipality cyber incidents. The first key similarity is that both events resulted in state emergency declarations, the first and third such declarations in history. The second declared event, in Louisiana, did not have sufficient information available to conduct a case study. Both of the events were coordinated at the state level with the assistance of state emergency management agencies. Part of the coordination involved bringing in other entities such as the National Guard/State Guard and the Department of Homeland Security. A final and significant similarity is that both events were ransomware attacks that rendered networks completely inoperable for a length of time with impacts in the physical world. In the case of CDOT, the Department of Transportation was unable to process transactions such as drivers' licensing and payroll, while in TX water utilities and law enforcement agencies were impacted.

Key differences in the events also impacted the response efforts. A significant difference between the two was the geographic footprint of response activities. In the CDOT incident the response was centrally located at the CDOT's IT facility, whereas the TX municipality incident occurred across the state in 23 municipalities. Coordinating resources in the two environments posed different challenges, particularly in communication and resource tracking. Communications were provided centrally with white boards and butcher paper in the CDOT incident, while the TX response team relied on digital communications tools separate from the impacted networks. There was also a difference in the involvement of political sub-divisions for the responses. In the case of CDOT, the primary response efforts occurred at the state level due to an impacted state agency. In Texas, the response efforts originated at the municipality level rather than the state, requiring coordination and collaboration with multiple government agencies on resource prioritization and action plans.

2. Common Terminology

The core concept of common terminology was clearly an issue in the CDOT ransomware attack but was not clearly identified as an issue or strength in the Texas ransomware event. In the CDOT event, the challenges attributable to unfamiliarity with terminology between cybersecurity and emergency managers were able to be worked through due to a trust relationship established from previously conducted joint exercises. An outcome of the incident is Colorado's OIT implementation of ICS/NIMS to ensure common terminology is used. This mirrors an outcome of the Texas incident, where the reporting recommends IT/CS responders complete all required TDEM training. The findings from the case studies are supported by the findings in the qualitative interviews.

Relevant Findings from Interviews

All four EM/HS leaders interviewed indicated a difficulty or expected difficulty creating a common understanding between EM/HS and IT/CS. As Director Willis stated, "there is still a cultural and communication gap between cyber and other responders. Three of the IT/CS leaders interviewed also referred to communication challenges associated with common terminology. Most notably, both Colorado and Texas are implementing ICS/ NIMS training for IT/CS responders as a result of their incidents.[126] Colorado has also begun working on rewriting their cyber incident response plan to include ICS/NIIMS principles.[127] While not specifically discussing the command and control of cyber response, CISO Ford emphasized the need in cybersecurity to implement common communications protocols within systems if there is to be successful integration. A significant observation by Deputy CISO Swanson was that a strength of ICS is its acceptance by responders in the physical world already. Swanson was also indicating, though, that this is a challenge to cyber incident response because IT/CS professionals generally do not speak the language now.

3. Integrated Communications

Integrated communications played a role in the ability to respond to the cyber incidents in both cases presented. In the Colorado incident, network incapacitation from the cyber attack resulted in the loss of the primary communications methods for the CDOT.

[126] Blyth, personal interview by author; Texas Department of Information Resources, "August Incident Hotwash #1 Outcomes" and Hahn, email message to author.

[127] Blyth, personal interview by author.

This hindered response efforts and caused the response information be shared in person on white boards and butcher paper. In the Texas incident, the geographic spread between impacted organizations proved the value of integrated communications for response. Responders used an online platform to share incident-specific information and for communications. This was identified as an area for improvement in the hotwash as a recommendation for a pre-identified communications platform for all agencies.

Relevant Findings from Interviews

The findings of the qualitative interviews support the case study findings. Six of the eight senior leaders interviewed discussed challenges with, or the importance of, integrated communications concepts. Deputy Director Sexton identified communications as a significant problem in a cyber incident in which his organization responded due to the inability to share files and information. This was also noted as a concern by Director Phelps, because there is always the potential during a significant cyber incident to knock communications offline. Three of the interviewees discussed the use of WebEOC software as an incident management platform as part of their response, but indicated that it would not be used for all horizontal and vertical communications in a response organization. In a 2020 recorded presentation to Secure World Atlanta on cyber incident response, CISO Allen pointed out that communication is still the toughest part of the response. His recommendations included that “overcommunication is key” and that response leadership needs to “feed the beast” in reference to sharing as much information as possible across stakeholder groups.[128] Using a more technical description of communication challenges for cybersecurity, CISO Ford noted the need in cyber incident response to automate whenever possible. He went on to describe how automation cannot occur until everyone is speaking the same language on the same tools. The explicit and implicit references to the challenges and recommendations for integrated communications suggest this concept as one of the most important of the eight core concepts.

[128] David Allen, “Ransomware Incident Command & Lessons Learned for Managers” (Secure World Atlanta, August 2020).

4. Modular Organization

The CDOT and Texas case studies both demonstrated the adoption of modular organizational concepts. Both states brought in external technical cyber resources as well as logistic support functions to their response structures. A resource that both used, for example, was state National Guard cyber teams.

Relevant Findings from Interviews

This application of modular organization concepts is supported by the qualitative interview findings. Both directors Schulz and Phelps described the appropriateness of ICS/NIMS in a cyber incident due to its scalability and flexibility in adding technical cyber response. Both directors also noted the applicability of the EM/HS ability to apply ICS/NIMS concepts to bring in other resources such as public information, logistics and planning expertise. One caveat that Schulz noted was the potential for conflict between a hierarchal organizational structure such as ICS/NIMS for IT/CS professionals who are more likely to be used to flatter organizational structures commonly associated with the IT/CS industry. Another concern with applying ICS/NIMS to significant cyber incidents by Director Willis was the immaturity of the framework for cyber events. In other disasters Willis describes responding as a "team of teams," while this has not been established for significant cyber incidents. Directors Willis, Schulz, and Phelps still advocate for the use of ICS/NIMS in these events due to the framework's developed processes for bringing in resources with different skillsets. The case studies and senior leader interviews both suggest that modular organization as a core concept is applicable as a concept in significant cyber response while acknowledging there are potential challenges to the implementation.

5. Recognized Command Structure

The core concept of recognized command structure was clearly a challenge in the CDOT incident and was implied in the Texas municipality cyber attacks. In the CDOT incident, there is a point of reference for response without the command structure provided by ICS during the first week and the contrasting response after the implementation of Unified Command. The Unified Command team addressed issues with response priorities, assigning of roles and responsibilities, and reducing friction among response organizations.

In the Texas incident there was no clear reference to the need for a central command overall. There were, however, findings in the case that suggest there were issues stemming from the lack of a central command structure at times. Two problems identified in the Texas case study were the need for a central reporting agency and the lack of a process to verify and authenticate response personnel. Coupled with the hotwash recommendation to complete recommended TDEM training, the identified problems suggest the desirability for a central coordinating command.

Relevant Findings from Interviews

The findings of the qualitative interviews suggest there is uncertainty in cyber events related to a recognized command structure. While all eight senior leaders recognized the need to establish common strategies and objectives, the effectiveness of ICS in its current form is still undetermined. While all the EM/HS leaders indicated that they believe ICS is an appropriate framework to apply, Director Willis acknowledged that the framework is not mature enough yet in cyber events. Similarly, all IT/CS leaders agreed that there needs to be a command structure, but only CISO Blyth specifically recommended ICS/NIMS. She noted the success of the Unified Command "keeping everyone in their lanes." Similarly, CISO Allen did not specify the use of ICS when discussing command and control but noted that EM/HS have a role at the macro-level similar to other disasters. Allen also conferred the importance of unity of command as a lesson learned during cyber incident response in his presentation to Secure World Atlanta.[129] In summary, a command that is unified in managing the objectives, strategies and priorities of an incident are viewed as essential.

6. Manageable Supervisory Structure

The case studies did not indicate the core concept of Manageable Supervisory Structure as an important factor in significant cyber incident response. Neither case revealed challenges with a span of control issue amongst responders with minor references to adequate distribution of subordinates in each case.

[129] Allen.

Relevant Findings from Interviews

The findings of the qualitative interviews support the concept that existing structures may already be adequate or that a manageable supervisory structure as an insignificant factor in cyber incident response. In the CDOT response, for example, Director Willis stated that span of control was not an issue as staff was already structured appropriately. ND CISO Ford pointed out that during a cyber response, the affordances of technology allow technical human resources to be spread further. As Ford said, “I think with the right tools and the right communication channels, I don’t really have much concern there.” Somewhat contrarian, EM/HS Director Cody Schulz did express concerns in his interview that an operations section within an ICS structure could get too big based on his experience in pandemic response. Schulz still believed that ICS/NIMS is applicable for maintaining proper span of control and that response leadership must remain flexible to fit the personnel structure and resources available. Overall, the core concept of maintaining a manageable supervisory structure is not indicated as substantial relative to the other core concepts for significant cyber incident response.

7. Consolidated Action Plans

There were several references to issues relating to the core concept of consolidated action plans in both cases studied. In the CDOT response it was clear that establishing a unified set of planning priorities by the Unified Command Group was one of the primary factors in the successful response. Prior to the establishment of the Unified Command Group, there was not a synchronized plan between business operations and the cyber response team, as well as challenges prioritizing and closing out tasks amongst responders. In the Texas response hotwash and incident response report there were references to the need to record meeting minutes and action plans, the acknowledgment of the coordinated plan legislation as a factor for their response success, the identification of triage, and prioritization.

Relevant Findings from Interviews

The findings of the qualitative interviews support this core concept as one of the more important concepts for application in significant cyber incident response. All of the interviewees specifically discussed the need to collaborate with stakeholders across fields of discipline, business units, and levels of government. The most common reason for the need to collaborate was to set priorities and allocate resources accordingly. As CISO Allen put it in his lessons-learned presentation, there is a need to mass resources on critical functions; known as "economy of force" in the military.[130] Allen's in-state EM/HS counterpart Deputy Director Mark Sexton agreed with the principal stating, "If you throw your bucket of water at the entire wall, it's going to get a little bit wet, but you're not going to put a fire out." Four of the interviewees also expressed concerns developing an initial common operating picture used in developing the action plans. As Director Schulz described the process: intel drives planning; planning drives response actions. Director Phelps specified that in a cyber incident, "information gets really locked up," which makes collaboration towards a unified objective difficult. The case study reviews and the qualitative interview findings support the concept of Consolidated Action Plans as a primary factor for successful response to significant cyber incidents.

8. Comprehensive Resource Management

The case studies revealed a close tie between the concepts of consolidated action plans and comprehensive resource management. Both the CDOT and Texas events used the resource management principles of ICS to bring in resources. The CDOT response required assets from vendors, state agencies, National Guard, FEMA, and Homeland Security while utilizing resource management tools such as EMAC, badging, and rest cycles for the human resources. Texas also had references to use of the resource tracking for reimbursement purposes as well as resource lists for available resources. In both responses, a statewide Emergency Declaration was issued by their Governors which opened the option for further resources and/or reimbursement of costs incurred.

Relevant Findings from Interviews

Most of the senior leaders agreed that resource management was a role that EM/HS leadership could help fill through the use of ICS/NIMS. In addition, there was consensus

[130] Allen.

that one of the most difficult problems to solve in a cyber incident is the lack of available technically trained human resources. CISO Allen, CISO Ford, and Deputy CISO Swanson all referenced difficulty determining what the specific resource needs are in each individual event and then finding the exact resources needed. An important facet of resource management was discussed by Allen in a lessons learned presentation in which he noted the necessity of providing the logistics for responders on scene and prepping the response site for arrival of the "main body."[131] In the CDOT event, CISO Blyth also noted this importance discussing items like providing food, beverages and sanitation.[132] In summary, there is overlap between the concepts of Comprehensive Resource Management, Consolidated Action Plans and Modular Organization, which makes it difficult to distinguish which of the three concepts are most significant.

9. Pre-Designated Facilities

There was minimal discussion of pre-designated facilities in the two response case studies. The CDOT case exposed a potential weakness of pre-designated facilities by response personnel unknowingly taking infected laptops to an uninfected network or vice-versa. Another newly discovered potential weakness pointed out by Colorado Director of Emergency Management Willis was a pandemic limiting the ability to have responders converge on a single location. Overall, however, the CDOT study highlighted the positive outcomes of having a SEOC to handle coordination of logistics and other second and third order effects in addition to the DOC providing a location for conducting business operations. The Texas case clearly and explicitly recognized the value of pre-designated facilities in the after action hotwash, recommending establishment of an identified and known multi-hazard event location for the cyber team. The Texas case also listed the use of the TDEM SOC as an important element of the response success.

[131] Allen.

[132] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack."

Relevant Findings from Interviews

Similar to the case studies, the qualitative interview findings had minimal discussion of the pre-designated facilities core concept. Only two EM/HS discussed the use of pre-designated facilities, and both referred to the value of sites separate from the response site to help coordinate logistics, second and third order effects, and to minimize distractions for on-scene responders. Two of the EM/HS leaders and one IT/CS leader discussed the likelihood that actual cyber response activities would occur on site, rendering the pre-designated facilities less important to the technical cyber response, and thus lowering the overall value of pre-designating response facilities. Even further diminishing the value of pre-designated facilities was CISO Ford's observation that in a cyber event there can potentially be a remote response from anywhere. As Ford stated, "a well-prepared organization can accept help from anywhere." In summary, the findings support the concept of pre-designated facilities as more applicable to coordinating efforts on second and third order effects and to providing logistical support to technical cyber responders. Conversely, the findings indicate that pre-designating facilities for the technical cyber response provides less value in a significant cyber incident.

10. Emergent Themes

There were two emergent themes from the case studies and one additional theme that was not evident in the case studies but apparent in qualitative interviews. In both case studies there were references to difficulties in developing a common operating picture and an expectation that EM/HS would join a cyber incident response to implement ICS for IT/CS. Beyond the two themes in the case studies, the interviews indicated a need for clarity as to what might constitute a cyber emergency versus a cyber disaster. These themes may have some practical ties to specific core concepts, but do not clearly link to any one of the concepts. Further, the emergent themes add to an overall understanding of the findings and the application of the core concepts in significant cyber incident response.

a. Establishing a Common Understanding of the Incident's Operating Environment

The first emergent theme that does not relate to one specific core concept is the difficulty establishing a common understanding of the incident's operating environment. Describing the CDOT response, Director Willis remarked that the biggest issue confronting the response leadership was the initial incident assessment across the cyber issues and the business functions. Director Phelps related the difficulty to a pandemic response, stating, "like COVID-19, very few people understand it." He went on to say that the resemblance between the two is due to an inability to see a virus or cyber incident as well as a relative lack of predictability compared to other natural disasters. The two other EM/HS interviewees, Schulz and Sexton, discussed the need to get timely and accurate intelligence about an incident in order to develop priorities, coordinate actions and assign resources. Sexton further related that developing a common operating picture was necessary to answer the question: "How big do I draw the box?"

The concerns with developing the common understanding are not limited to the EM/HS professionals. The IT/CS leaders interviewed also discussed this as a key issue. CISO Allen noted that the first step in a cyber incident response is building the common operating picture.[133] Some of the key issues associated with communication in a significant cyber incident according to Allen are not being notified of an incident soon enough and not having a good common operating picture to choose resources and set priorities. CISO Blyth also discussed the difficulties of understanding and synching the issues between the business functions and the cyber incident response efforts during the CDOT response.[134] Acknowledging that a complete understanding of the situation is unlikely in a significant cyber incident, Deputy CISO Swanson observed that leaders will have to make the best decisions they can with the data they have at hand. The numerous references to the challenge of developing a common operating picture in a significant cyber incident indicate an important opportunity to improve response efforts.

[133] Allen, "Ransomware Incident Command & Lessons Learned for Managers."

[134] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack."

b. ICS Framework Wrapper

Another finding of the qualitative interviews was the universal expectation that EM/HS professionals would join an incident response and wrap the ICS framework around the technical IT/CS response efforts. EM/HS Directors Phelps and Schulz both indicated that this is common based on past experiences in other significant (non-cyber) events where the emergency management agencies have been brought in to organize response efforts, even though they were not the experts in the specific incident area such as pandemic or civil unrest. The two indicated that the EM/HS expertise in disasters are organization and an ability to coordinate amongst competing priorities and second or third order effects. Director Willis noted that in the CDOT incident, even if responders hadn't been trained on ICS, the EM/HS professionals were able to explain what was going on from an ICS standpoint and the IT/CS responders were able to understand it. The IT/CS leaders interviewed indicated that their expectation was that emergency management organizations would be able to integrate cyber operations into a broader response framework that considered the second and third order effects. CISO Ford noted that one of his areas for concern in a significant cyber incident was when the incident was part of another incident such as a flood, pandemic, or fire, which is when he would rely on EM/HS to implement ICS. Deputy CISO Swanson used the terms "defer to you," referencing an expectation that IT/CS would rely on EM/HS to implement the ICS framework around the cyber response command and control structures. Further bolstering this finding, CISO Allen discussed, based on his response experiences, that the purpose of the leadership in a significant cyber event was to take care of the macro-level interagency coordination in order to provide top-cover for the technical responders to handle their specific response tasks. In short, due to a lack of ICS trained IT/CS personnel, there was an expectation that EM/HS would be able to provide an overarching ICS structure.

Although the findings supported the expectation of a "wrap around" ICS capability by EM/HS professionals, there was still support for cooperative pre-incident training and exercises between EM/HS and IT/CS responders. First, relating to ICS, there was support for some level of basic ICS/NIMS training for cyber responders. Director Schulz noted that he considers the lack of ICS training by technical responders in the COVID-19 pandemic as a weakness in current response efforts and expects a similar problem to arise in significant cyber incidents. Director Willis remarked that once there is a framework, training can occur around it. Similarly, there were recommendations in the interviews for EM/HS responders to receive training on basic cybersecurity and information technology principles. CISO Blyth recommends cyber training for EM/HS responders but also noted that even without the training the ICS framework is useful. Among those who discussed cross-training amongst disciplines as described above, there was not an expectation that either group needed to become experts in another field, but rather to learn just enough to be able to understand the basic principles and terminology of ICS/NIMS and cybersecurity. Beyond training, a common recommendation amongst the senior leaders for the other disciplines was to participate in joint exercises. The basic commonality between the exercise recommendations was for EM/HS responders to integrate cyber into exercises and for IT/CS responders to integrate ICS into cyber exercises. In the case of Colorado and CDOT, Director Willis lamented that even though they had conducted exercises between the IT/CS and EM/HS groups, they did not incorporate ICS/NIMS into the exercises. “That was a mistake,” Willis said.

c. Distinguishing Between a Cyber Emergency and a Cyber Disaster

One of the underlying challenges of the research was distinguishing between a cyber emergency and a cyber disaster. Each interviewee seemed to have a different perception on when a cyber incident became a significant cyber incident that required the need to bring in additional command and control elements. One common perception is when a cyber incident moves beyond networked systems and has impacts in the physical world, or when there is an incident in the physical world impacting IT systems. This was referred to by multiple key leaders as second or third order effects in the interviews. Another criterion is when internal response resources are exhausted and external resources are required. A final criterion that emerged was simply when the response goes beyond the routine incident capabilities of the organization. This final criterion reflects a key part of the definition of disaster provided in Disaster Response, which includes the verbiage "cannot be managed through the routine procedures and resources of government."[135] The findings also echo Disaster Response's differentiation between emergencies and disasters by the changes in the division of labor and resources from routine emergency management.[136] Clarifying the distinction between when a cyber emergency becomes a cyber disaster may prove useful in future analysis and research of the application of ICS in significant cyber incident response, but it was not a primary goal of this research.

11. Summary

The case studies supported the application of the core concepts of ICS in a significant cyber incident. The differences in the two incidents relative to geographic area, communication challenges, and breadth of stakeholders are indicative of broader application of ICS for response efforts in similar incidents. Applying the core concepts of common terminology, integrated communications, modular organization, recognized command structure, consolidated action plans and comprehensive resource management are all supported by the qualitative findings. The concept of pre-designated facilities for the technical cyber response was not strongly supported by the findings; however, there were indications that pre-designated facilities are still useful for coordinating response to the second and third order effects. Maintaining a manageable supervisory structure as a core concept was not supported by the findings. Further findings indicated a difficulty and high importance of establishing a common operating picture in significant cyber incidents. Another emergent theme was the expectation that EM/HS professionals would be able to implement an ICS framework around IT/CS response measures, to mitigate a shortage of ICS trained IT/CS personnel. The final emergent theme from the qualitative interviews was the need to distinguish when a cyber emergency becomes a cyber disaster, requiring the escalation of response efforts to include a more robust response framework. Overall, the findings support ICS/NIMS as a framework for organizing response efforts for significant cyber incidents.

[135] Auf der Heide, Disaster Response: Principles of Preparation and Coordination, 51.

[136] Auf der Heide, 53.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERCEPTIONS OF ICS ORGANIZATIONAL RESPONSE CHARACTERISTICS IN SIGNIFICANT CYBER EVENTS

A. METHOD

This chapter examines the results of an anonymous online survey of potential cyber incident responders from the EM/HS and IT/CS fields. Using Burgiel's eight core concepts of ICS and demographic data to separate participants into subgroups, the survey evaluates perceptions of organizational response characteristics in significant cyber incidents. This chapter will first show a breakdown of the population group's demographics, including which subsets of data proved relevant. Next, an in-depth evaluation of the survey results for each of the eight core concepts is presented in conjunction with the relevant qualitative findings from the semi-structured interviews to enhance the understanding of the survey results. As in the case study chapter, the interviews were first deductively coded to the eight core concepts of ICS as defined by Burgiel.[137] After each core concept has been analyzed, a comparative means analysis is conducted to provide further insight into each field's perception of ICS application. The chapter closes with a brief summary of the results and findings.

B. DEMOGRAPHICS

The total quantitative sample (TS) for analysis included 79 records which were able to be analyzed across multiple subgroups. Five demographic subgroups were evaluated including respondent field of work, incident experience, work experience, career level, and organizational type. Table 3 highlights the specific categories within each subgroup. In order to test the hypothesis that ICS/NIMS can be used to improve significant cyber incident response, this study assumes that EM/HS professionals have a significant experience advantage using ICS/NIMS over IT/CS professionals. It is an assumption of this research that the longer a survey respondent has been in his or her field, the more knowledgeable the respondent will be about how his or her organization and other similar

[137] Burgiel, "The Incident Command System," 158; Department of Health and Human Services, "Overview of MSCC, Emergency Management and the Incident Command System."

organizations would respond to a significant cyber incident. All of three subgroups provide statistically significant results for further analysis. A consolidated table of individual survey responses can be found in Appendix C.

Table 3. Quantitative Subgroups for Analysis

Subgroups	Number (*n*)	Percentage (*%*)
Total Quantitative Sample (TS)	79	100%
Emergency Management/Homeland Security (EM/HS)	48	61%
Information Technology/Cybersecurity (IT/CS)	31	39%
No Response Experience (NR)	35	44%
Yes Response Experience (YR)	44	56%
Less than 5 Years Experience In Field (<5)	9	11%
5 or More Years Experience In Field (≥5)	70	89%
Practitioner (PR)	17	34%
Mid-Management (MM)	27	22%
Senior Leadership (SL)	35	44%
Government (GO)	67	85%
Private Sector (PS)	10	13%
Other (OT)	2	3%

Two additional subgroups are analyzed for statistical significance. The career levels (Level) of study participants were categorized as Practitioner (PR), Mid-Management (MM), and Senior Leadership (SL). Survey participants self-selected their career level during survey completion. The population pool of these categories is 17, 27, and 35 respectively. The final subgroup of organizational affiliation (Organization) is divided among three categories, Government (GO), Private Sector (PS), and Other (OT). The relative numbers of each category are 67 (GO), 10 (PS), and 2 (OT). Relative to the "Other" and "Private Sector" subgroups, who made up 3 and 13% each, this sample pool heavily favors a government organization perspective. This may be viewed as a weakness or a strength of the study, depending on the reader's perspective. The results of the data analysis may be more applicable to government agencies than their private sector and other counterparts. Private sector and other organizations that routinely, or expect to in the future, interface with government-led response efforts may also find the analysis more useful. Neither the Level nor the Organization subgroups provided any statistically significant results relative to the eight core concepts. It should be noted, though, that there are indications that these demographics may provide other useful data. The TS proved sufficient for providing statistical relevance during analysis. Additional time and recruitment resources would have likely improved both the quantity and quality of data.

C. SURVEY EVALUATIONS BY CORE CONCEPT

1. Common Terminology

a. Quantitative Analysis

The following analysis in Table 4 describes the results for the core concept of common terminology. Analysis of the Field group, Incident subgroup, and Experience subgroup all returned statistically significant results. The table also includes the full population sample's pool size (*n*), *M*, and *SD* for reference. Of the eight core concepts, it had the greatest number of statistically significant results. The questions in the survey included both the positive (+) and negative (-) indicator statements below:

> + *My organization uses common terminology during significant cyber incident response that is easily understood by outside agencies.*
>
> - *Common terminology that is easily understood by external organizations is not used by my organization during a significant cyber incident response.*

Table 4. Common Terminology Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	5.12	1.39				
Field	EM/HS IT/CS	48 31	4.84 5.55	1.39 1.30	1	2.26	5.10	.027
Incident	NR YR	35 44	4.66 5.49	1.36 1.31	1	2.75	7.57	.007
Experience	<5 yrs ≥5 yrs	9 70	6 5.01	1.09 1.39	1	-2.06	4.24	.043

Note: *95% Confidence interval used for calculating *p* values.

The first statistically significant result revealed was related to the field of discipline category of responses. The mean of responses for EM/HS participants (*M* = 4.84) rates most closely to Somewhat Agree for their organizations' use of common terminology that external agencies understand. IT/CS respondents rated their organization's use of common terminology higher (*M* = 5.55), which rounds up to Agree on the Likert-scale. The statistically significant *p*-value (*p* = .027) supports the perception that IT/CS responders believe they use common terminology that is more easily understood by outside stakeholders than their EM/HS counterparts. This may be explained by IT/CS professionals using a common language that is understood by those in their field, which is a pre-requisite for making computer networks function. IT/CS terminology has very specific meanings that EM/HS professionals do not understand but is common in the IT/CS field.

The second area of means analysis that proved statistically significant is the perception of common terminology between significant cyber incident response experience (Incident). Survey participants who have this experience rate their organizations higher (*M* = 5.49) than those without response experience (*M* = 4.66). While both would technically rate as Somewhat Agree on the Likert-scale due to rounding, those with experience were at the very top of the category while those who did not were at the bottom. The statistically significant *p*-value (*p* = .007) indicates that prior experience responding to a cyber incident raises the perception that an organization uses common terminology that external agencies understand.

The final statistically significant subgroup for common terminology is the respondents' length of time in their fields (Experience). The <5 category rated their organizations' use of common terminology higher (*M* = 6) than the ≥5 category (*M* = 5.1). The *p*-value is statistically significant at *p* = .043. If one were to assume that those with less experience were also less likely to have been involved in a previous significant cyber incident response, one may conclude that "they don't know what they don't know." The evidence points to experiential learning from a previous response as a factor that would increase average scores for common terminology. Conversely, experience in the field reduces the average scores. Another possible explanation for this result could be based on an assumption that those with more experience have worked in multi-agency environments where collaboration revealed challenges with developing a common understanding. Participants who have had that experience may be more self-aware and lowered their scores accordingly. Similarly, the evidence suggests that this may explain the lower rating of common terminology by EM/HS participants than IT/CS.

b. Relevant Qualitative Findings

The qualitative findings support the quantitative results for common terminology when considering the participants field of discipline. The results may be indicative of specific terminology used in the IT/CS field which is necessary to make networks function. Therefore, it may be assumed that IT/CS practitioners are forced to use specific, common language amongst their own field while still being difficult to understand by the EM/HS field. Seven out of the eight leaders interviewed noted the challenge of communicating in ways so the various stakeholders can understand the situation. This can result in a difficulty establishing a shared understanding, according to ND Homeland Security Director Cody Schulz. One emergency management director noted that during sensitive cyber briefings the "digestibility of what can be shared" made understanding the threats difficult and it was as if they were "speaking a different language."[138] Colorado's Director of Emergency Management Mike Willis described a lesson their responders learned during their response to the Colorado Department of Transportation described in the case study in Chapter 2. He noted that cyber people are really technical, and the emergency managers let them get away with not collaborating because they are intimidated by the technological nature of the incident. "It's not a cyber thingy, it's an incident" is how he describes the challenge to emergency managers.

The qualitative findings did not support nor disprove the quantitative results for previous incident response experience and the use of common terminology. This is likely due to no specific questions being asked about experiential learning. The quantitative results do support that experiential learning has an impact on an organization's use of common terminology. One may consider that there are two ways to learn about disaster

[138] Andrew Phelps, personal interview with author, Microsoft Teams Video meeting, October 10, 2020.

response, training, and exercise or on-the-job training. As Mark Sexton, Deputy Director of Programs and Finance for the Georgia Emergency Management and Homeland Security Agency (GEMA), puts it: “Everyone is a culmination of their previous experiences.” He went on to recommend that IT/CS and EM/HS organizations build relationships and learn to understand each other’s terminology in blue-sky days, because the gray-sky day is too late. Further, 7 of the 8 interview participants indicated support for cross-training and/or exercises between EM/HS and IT/CS professions so that they would better understand each other. A key comment by Director Willis noted that prior to the CDOT ransomware attack, the cyber exercises that the organizations had worked on together did not include ICS/NIMS. “That was a mistake,” Willis said.

c. Summary

The statistical analysis of the common terminology core concept reveals some interesting phenomena. Overall, the evidence supports the concept that previous response experience raises an organization’s ability to use common terminology in a significant response. Additionally, the results indicate that experience with incident response in general may increase self-awareness that an organization’s common terminology is not understood by external organizations. Qualitative findings also strongly suggest that using common terminology is a significant issue during cyber response activities when multiple agencies are involved. As Director Willis explained, “There is still a cultural and communication gap between cyber and other responders.” His state counterpart, Chief Information Security Officer Deborah Blyth, agreed and indicated that their agencies are currently re-writing their state’s cyber incident response plan in an ICS/NIMS format so the whole group is “speaking the same language.”

2. Integrated Communications

a. Quantitative Analysis

The analysis of the Integrated Communications concept is represented in Table 5. Analysis of the Field group and Incident subgroup are included; however, only the Incident subgroup returned statistically significant results. The questions in the survey included both the positive (+) and negative (-) indicator statements below:

+ My organization uses a common communications plan that has interoperable processes and systems for coordinating with external agencies during significant cyber incident response.

- My organization does not use a common communications plan, interoperable communications processes, or interoperable systems during significant cyber incident response.

- My organization does not have an existing plan to ensure common systems and processes for communications are in place with external and internal stakeholders.

Table 5. Integrated Communication Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	5.19	1.15				
Field	EM/HS	48	5.08	1.22	1	1.05	1.11	.296
	IT/CS	31	5.35	1.03				
Incident	No	35	4.84	1.24	1	2.48	6.14	.015
	Yes	44	5.46	1.00				

Note: *95% Confidence interval used for calculating *p* values.

The Field subgroup results are not statistically significant in this core concept. The *p* value of .296 falls just outside the 95% confidence internal. EM/HS respondents rated their organizations' weaker (*M* = 5.08) at using integrated communications compared to their IT/CS counterparts (*M* = 5.35). This was one of four concepts in which IT/CS rated their organizations higher than EM/HS. These results suggest that integration of communication platforms is already a generally accepted principal across both disciplines, with both fields of discipline somewhat agreeing that their organizations use integrated communications as part of their cyber incident response efforts.

Statistical significance did result in the Incident subgroup analysis (*p* = .015). Respondents with prior experience in significant cyber incident response rated their organizations' use of integrated communications higher (*M* = 5.46) than those without that experience (*M* = 4.84). The evidence suggests experiential learning can raise an organization's implementation of integrated communication technologies and processes.

b. Relevant Qualitative Findings

The idea that integrated communications are already an accepted principle in both EM/HS and IT/CS is supported by the qualitative findings. In EM/HS, a lack of integrated communications was recognized as a significant problem during the response to the September 11, 2001, terrorist attacks.[139] Since then, a substantial effort has been made to increase integration of communications through the use of Homeland Security Grant funding.[140] In the information technology fields, desire for integration is ubiquitous. CISO Kevin Ford discussed this in depth in his interview, noting that in cybersecurity, "first you integrate, then you automate." Ford went on to say: "You integrate then you automate right? So, you have to pre-negotiate, but once everyone's speaking in the same language on the same tools, then you can automate." He further detailed that in cyber incident response, wherever possible an organization should look to automate.

The results of the prior incident response analysis are neither supported nor contradicted by the qualitative findings. No specific qualitative questions were asked regarding how prior incident response has affected the organizations' implementation of integrated technologies and processes for cyber incident response. Interestingly, three of the four EM/HS leaders interviewed discussed the challenges of losing the capability to coordinate and communicate due to systems being impacted by the cyber event. This may indicate that integrated communications are a weakness during a significant cyber incident where no redundancy in technology or process exists. As seen in the Colorado CDOT case study, the impacted systems would have otherwise been a part of the integrated systems used in response. This resulted in the need to co-locate response assets and the use of butcher paper and white boards for communication before additional communications systems could be implemented.[141] Director Willis went on to note during his interview

[139] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: The National Commission on Terrorist Attacks Upon the United States, 2004), 319, 414, https://govinfo.library.unt.edu/911/report/911Report.pdf.

[140] U.S. Department of Homeland Security, The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO)Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP) (Washington, DC: Department of Homeland Security, 2020), 17, 21, 26, https://www.fema.gov/sites/default/files/2020-08/fema_homeland-security-grant-program-nofo_fy-2020.pdf.

[141] Bismarck State College, College Relations, "Key Takeaways from the 2018 Ransomware Attack."

that this response occurred pre-COVID-19, indicating that in a pandemic environment co-locating during response may not be an option for redundancy.

c. Summary

The analysis of the Field subgroup was not statistically significant while the Incident subgroup did provide important results. The alignment of means in the field of discipline suggests that integrated communications are already ubiquitous in both fields. This is supported by the qualitative findings discussing the use of integration and automation in IT/CS as well as the effect of the 9/11 Commission recommendation to integrate communications systems. Relative to the Incident subgroup, the quantitative findings once again suggest that experiential learning raises the perception of increased implementation of integrated communications as a core concept. The qualitative findings for the Incident subgroup, neither supported nor contradicted the quantitative results. Rather, the qualitative findings suggest that a loss of integrated communications during a significant cyber incident is a substantial concern for EM/HS leaders.

3. Modular Organization

a. Quantitative Analysis

The core concept of the Modular Organization is detailed in Table 6. The analysis of the Field group and Experience subgroup are both included for further discussion. The Field group did not provide statistically significant results (*p* = .739); however, the Experience subgroup was statistically significant (*p* = .040). The survey questions for Modular Organization follow, including both positive (+) and negative (-) indicator statements:

> *+ During a significant cyber incident response, my organization takes a modular approach that allows it to expand to include additional internal and external stakeholders.*
>
> *- My organization's structure is not designed to expand or contract based on the complexity when responding to a significant cyber incident.*

Table 6. Modular Organization Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	5.20	1.42				
Field	EM/HS	48	5.24	1.55	1	-.33	.11	.739
	IT/CS	31	5.13	1.22				
Experience	<5 yrs	9	6.11	.74	1	-2.09	4.37	.040
	≥5 yrs	70	5.08	1.45				

Note: *95% Confidence interval used for calculating *p* values.

The analysis of means for the Field subgroup was not statistically significant (*p* = .739) in the Modular Organization core concept. EM/HS respondents rated their organizations’ use of modular organization concepts slightly higher (*M* = 5.24) than their IT/CS counterparts (*M* = 5.13). Both groups somewhat agree that their organizations’ use modular organization concepts, with little difference between the two fields. The results indicate that the ability to add and remove different organizations to a response team during a cyber incident is already equally accepted by both groups.

The only statistically significant result for the Modular Organization concept is the Experience subgroup (*p* = .040). Survey respondents with less than five years of experience in their field rated their organizations’ ability to scale a response team higher (*M* = 6.11) than those with five or more years (*M* = 5.08). The less experienced group rated agreed that their organizations adapt concepts in their response frameworks that allow for easy integration of stakeholders, while those with more experience only somewhat agreed. The difference in means of 1.03 was the highest separation amongst the subgroups in the analysis of all concepts, indicating a larger gap in perceptions. Under the assumptions that those with more experience are increasingly likely to have been involved in a previous incident, as well as have more experience working on projects involving internal and external stakeholders, the results may indicate that the <5 respondents simply “don’t know what they don’t know.” Conversely, although the results were not statistically significant (*p* = .084), those with incident response experience rated their organizations higher at applying modular organizational concepts (M = 5.44) than those without response experience (M = 4.89). Further, the results may indicate an increased willingness and flexibility by those new to the field to collaborate with other stakeholders. The results are inconclusive for the Experience subgroup.

b. Relevant Qualitative Findings

Qualitative findings related to the Modular Organization concept support the quantitative results for the Field subgroup. The qualitative interviews did not help to explain why EM/HS and IT/CS professionals are similar in their use of modular organization concepts but, rather, identified the shared idea of the importance of working with the different stakeholders. Six of the eight senior leader interviews made a reference that applied to modular organization. One of the clearest examples of modularity being implemented was discussed in the CDOT case study. Both Director Willis and CISO Blyth referenced how important it was to bring in the National Guard, DHS and FEMA assets as the response effort grew beyond Colorado’s capability. Willis and Blyth also noted the challenges of incorporating vendors into a unified approach to a cyber response due to competing priorities from the Unified Command and competition amongst vendors. Another example of modularity’s importance was noted by EM/HS Directors Andrew Phelps and Cody Schulz discussed the use of ICS/NIMS as a good support function for managing the second and third order effects of a cyber incident. One of the common sayings in disaster response is that disasters begin and end locally.[142] CISO Kevin Ford notes the challenge of returning an incident back to the local level in a significant cyber incident due to the non-technical issues of victim notification, public information, etc.

There were no qualitative findings related to the results of the Experience subgroup analysis. No specific questions were asked relating to how the length of experience in the field of discipline might impact the perceptions of an organization’s use of modular organization concepts. The lack of qualitative findings to support or contradict the quantitative analysis results in an inconclusive analysis of the subgroup.

[142] Federal Emergency Management Agency, *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101* (Washington, DC: Department of Homeland Security, 2010), 4–5, https://www.ready.gov/sites/default/files/2019-06/comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans.pdf.

c. Summary

The Field subgroup was not statistically significant, so the evidence is unable to conclusively support any hypothesis. What it may suggest is the necessity and ability of adding additional stakeholders to a significant cyber response is already an accepted priority in both fields of discipline. The Qualitative findings support the results with the majority of leaders interviewed acknowledging the importance of coordinating external stakeholders as part of the response. Specific to ICS, Director Willis of Colorado concluded that in other disasters EM/HS respond as part of a "team of teams" with other organizations. Unfortunately, he also noted that the field has not developed that same capability yet with significant cyber incident response. The results of the Experience subgroup were unable to be supported with any qualitative findings; however, the results may indicate either the less experienced respondents "don't know what they don't know," or that the more experienced group is less willing and able to incorporate other stakeholders into response efforts. The Experience results and findings are inconclusive.

4. Recognized Command Structure

a. Quantitative Analysis

The Recognized Command Structure concept analysis in Table 7 only includes the Field group. There were no statistically significant results for the Command Structure group (*p* = .220). The Field group results are included for further analysis. The following survey questions were included, indicating both positive (+) and negative (-) versions:

> (1) + *During incident response, my organization's processes are designed to incorporate multiple organizations in the adoption of goals, strategies and action plans to minimize duplication of efforts.*
>
> (2) - My organization's incident response framework is not designed to incorporate other external stakeholder leadership in a unified command approach.

Table 7. Recognized Command Structure Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	5.51	1.20				
Field	EM/HS IT/CS	48 31	5.65 5.31	1.16 1.24	1	-1.24	1.53	.220

Note: *95% Confidence interval used for calculating *p* values.

For the Recognized Command Structure core concept, EM/HS rate their organizations higher (*M* = 5.65) than IT/CS by a small margin (*M* = 5.31). The small margin and higher *p*-value indicate that both fields of discipline value a unified command structure. Additionally, the overall results (Sample *M* = 5.51) support this core concept as the highest perceived strength amongst respondents.

b. Relevant Qualitative Findings

All eight senior leaders interviewed recognized the need to establish common strategies and objectives during significant cyber incident response. This undivided response supports the quantitative results. The EM/HS leaders all seemingly supported a Unified Command structure using ICS/NIMS doctrine as a foundation when there were second and third order effects to be managed. Additionally, three of the four IT/CS leaders described a role for an ICS/NIMS command structure under the same response conditions. CISO Allen described the need for leadership to remain flexible in a significant cyber incident response because responders are dealing with an adversary and there are likely to be second and third order effects.[143] Director Phelps described one of the related challenges in a significant cyber event as a lack of clear lines of authority in a cyber incident. His comment was unknowingly addressed by Deputy CISO Swanson, who stated that, "one of the strengths of ICS is that it provides a known, clear chain of command, and it is very clear in its processes." Further expanding on his comment, Swanson

[143] Allen, "Ransomware Incident Command & Lessons Learned for Managers."

acknowledged the need for a command structure but cautioned that there should be guidelines for significant cyber responses, and everyone needs to agree to them.

The lone interviewee who did not mention ICS/NIMS or a unified command structure, CISO Ford, did discuss issues with command and control when other organizations or response functions were involved. For example, Ford noted that the IT/CS professionals will fix the technical problem, but there are still business problems that need to be addressed by others, such as victim notification and public information. Key to the line of discussion on command and control for CISO Ford was the use of automation in cyber incident response whenever possible. According to Ford, "the most effective command and control is automation." Ford's comments were not meant to support or contradict the use of ICS/NIMS in cyber incident response, but rather to emphasize the use of automation of processes wherever possible.

c. Summary

The results of the analysis did not provide strong evidence for the Field subgroup as it relates to the recognized command structure concept. The results were not statistically significant. What the results may support is an overall high value placed on command structure in both professional fields. Both EM/HS and IT/CS rated their organizations highly at implementing the concepts, resulting in the highest combined mean across all reviewed concepts. The qualitative findings support the results indicating that organizations in both fields are already recognizing the need to collaborate and coordinate with other agencies in significant cyber response.

5. Manageable Supervisory Structure

a. Quantitative Analysis

The analysis of the Manageable Supervisory Structure concept is represented in Table 8. Only analysis of the Field group was included for further discussion; however, no subgroups returned statistically significant results. The questions in the survey included both the positive (+) and negative (-) indicator statements below:

+ As a general rule, my organization has procedures in place to ensure supervisors do not have more subordinates than they can manage during a significant cyber incident.

- There is no plan or policy in my organization to ensure that supervisors maintain a manageable number of subordinates during incident response.

Table 8. Manageable Supervisory Structure Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	4.60	1.42				
Field	EM/HS	48	4.57	1.47	1	.22	.05	.827
	IT/CS	31	4.65	1.36				

Note: *95% Confidence interval used for calculating *p* values.

The results of the analysis for the Manageable Supervisory Structure were the second of three concepts that IT/CS rated their organizations higher (*M* =4.65) than the EM/HS group (*M* =4.57). The mean difference between the two, coupled with the high p-value indicates that there is minimal difference in the perception between EM/HS and IT/CS relative to their organizations' use of manageable supervisory structure concepts in cyber incident response. Interestingly, this core concept was the lowest rated concept amongst the eight both individually by field of discipline as well as combined (Sample *M* = 4.60). The evidence suggests that both groups value the concept roughly the same, but that value is lower than the other eight core concepts.

b. Relevant Qualitative Findings

The qualitative findings support the results of the Manageable Supervisory Structure core concept. There was minimal discussion of this concept during qualitative interviews, but when asked directly a few notable points were made. Director Willis said that during the CDOT response, span of control was not an issue because the teams were already structured appropriately. He did, however, claim that prior to EM/HS getting involved and implementing the ICS framework the CISO Deb Blyth was probably working beyond her own span of control. Specifically, he noted that CISO Blyth was taking on too many non-technical roles such as logistics instead of focusing on the technical information technology response she was charged with leading. Blyth acknowledged this in a conference presentation and also added in her interview that ICS was successful in structuring personnel so that leadership knew where they were.[144] North Dakota CISO Kevin Ford conferred in his interview that in a significant cyber incident response assistance could be accessed remotely and more quickly than in a traditional natural disaster. “I think with the right tools and the right communication channels, I don’t really have much concern there,” Ford said, discussing span of control in a cyber event. He also made the claim that automation in cybersecurity has allowed the expansion of span of control because technology can take care of more menial cybersecurity tasks, raising the opportunity for humans to focus on important tasks. Director Schulz also made a point regarding the culture of IT/CS organizations as having a flatter structure compared to more traditional hierarchal organizations represented in disaster response. During a cyber response, Schulz did have concerns that operations sections may grow too large, as was a problem during pandemic response.

c. Summary

The Field subgroup was not statistically significant in the Manageable Supervisory Structure core concept, so the evidence does not clearly support any conclusions. What it may suggest is an equal value placed on the core concept by both EM/HS and IT/CS. With both fields rating the concept lowest (M = 4.60) among the eight core concepts, the results indicate that EM/HS and IT/CS organizations place less emphasis on this concept during significant cyber incident response. The qualitative findings support the results of both a similar value placed on the concept by the two fields of discipline and the lower overall value of the core concept as part of significant cyber incident response.

[144] Bismarck State College, College Relations, “Key Takeaways from the 2018 Ransomware Attack.”

6. Consolidated Action Plans

a. Quantitative Analysis

The core concept of Consolidated Action Plans is detailed in Table 9. The analysis of the Field group and Experience subgroup are both included for further discussion. The Field group did not provide statistically significant results (*p* = .889); however, the Experience subgroup was statistically significant (*p* = .045). The survey questions for Consolidated Action Plans follow, including both positive (+) and negative (-) indicator statements:

> *+ During a cyber incident response my organization collaborates with other agencies to create a single, formal document stating incident goals, objectives, and strategies.*
>
> *- When responding to a significant cyber incident involving multiple organizations, there is no formal mechanism in my organization to ensure a unified set of strategies, objectives and goals is incorporated.*

Table 9. Consolidated Action Plans Descriptive Statistics and ANOVA

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	4.90	1.40				
Field	EM/HS	48	4.92	1.43	1	-.14	.02	.889
	IT/CS	31	4.87	1.37				
Experience	<5 yrs	9	5.78	.91	1	-2.04	4.16	.045
	≥5 yrs	70	4.79	1.42				

Note: *95% Confidence interval used for calculating *p* values.

The results of the analysis of means in the Field subgroup were not statistically significant. Of all the core concepts, this had the most closely aligned Field subgroup with a mean difference of .05. This indicates that both EM/HS and IT/CS organizations equally understand and value the need to provide formal, coordinated goals, objectives and strategies during significant cyber incident response. Additionally, these goals, objectives and strategies should come from a process of collaboration amongst stakeholders. Both groups scored their organizations relatively low (*M* = 4.90) in their use of consolidated action plans, which supports a concept that these organizations have room for improvement.

The only statistically significant results from the Consolidated Action Plans core concept were in the Experience subgroup. As seen in previous Experience subgroup analysis, the results show that those with less than five years' experience rate their organizations' use of consolidated action plans higher (*M* = 5.78) than those with at least five years (*M* = 4.79). While not statistically significant (*p* = .231), the mean of those with prior significant cyber incident experience (*M* = 5.07) was greater than those without response experience (*M* = 4.69). The results of the two subgroups contradict each other if there is an assumption that those who have more time in the field are more likely to have been part of an incident response. This may indicate that those with less experience are overly optimistic in their organizations' ability to create a formal consolidated action plan during a significant cyber incident response. Simply put, they may not know what they think they know.

b. Relevant Qualitative Findings

The results of the quantitative analysis of the Field subgroup are supported by the qualitative findings. Seven of the eight qualitative interviews discussed concepts related to consolidated action plans, with common themes of challenges in developing a common operating picture to set priorities and coordinating actions between business functions and response functions of organizations. Texas Deputy CISO Swanson acknowledged that one of the most significant challenges of a cyber response is prioritizing business needs with other needs such as preservation of evidence and getting networks back up and running. Further supporting a weak spot in significant cyber incident response, Director Schulz discussed that using ICS/NIMS in a cyber incident is expected to be more difficult because IT/CS professionals do not use ICS/NIMS frequently in their operations as compared to traditional responders like police, fire, and emergency management. Schulz went on to say that this has been a challenge in pandemic response as technical health workers are not trained and do not routinely use ICS/NIMS. While not contradicting the seven other leaders, CISO Ford focused setting the priorities of action as much as possible using automation. The need to develop priorities in action plans was documented in both AARs for the CDOT and Texas Municipality events described in the case studies.[145]

Quantitative findings support the quantitative analysis regarding the challenge of formulating consolidated action plans due to difficulties establishing a common operating picture. As Director Phelps stated about cyber incidents in his interview, “information gets really locked up.” Expanding on that, Director Schulz discusses how the inability to develop that common operating picture through intelligence process disrupts the planning process which in turn determines response actions. In discussing the CDOT cyber attack, CISO Blyth remarked that the ICS structure allowed the command team to first prioritize and second close out tasks, which aided in prioritization of resources. Her counterpart, Director Willis, compared response to significant cyber incidents with other natural disasters by stating that the first thing needed is an initial assessment of the consequences and incident factors to scope the incident and then prioritize actions.

The qualitative findings for the Experience subgroup do not strongly support or contradict the quantitative results. No questions were asked relating to the length of time in their field and their perceptions of consolidated action plans during the senior leader interviews. Taken as a whole, the findings from interviews and case studies do suggest that those who have been involved in a significant cyber incident response have acknowledged difficulty in creating consolidated action plans due to an inadequate common operating picture or competing business and response priorities. Without specific qualitative data from a related sample population, these findings remain inconclusive.

c. Summary

In summary, the Field subcategory was not statistically significant unlike the Experience subgroup. The results of the analysis on the Field subcategory provide weak evidence to support the notion that consolidated action plans are an ongoing challenge for both EM/HS and IT/CS due to a high *p*-value. A relative low mean for both groups for this

[145] Colorado Department of Transportation, *CDOT Cyber Incident*, 8; and Texas Department of Information Resources, “August Incident Hotwash #1 Outcomes.”

core concept supports that assertion. The findings show one of the drivers of the perceived weakness is an inability to develop a common operating picture to set priorities needed to develop the action plans. The Experience subgroup is statistically significant and may suggest that those with less experience in the field simply do not know what they don't know. The results of the Incident subgroup analysis and the qualitative findings from case studies and senior leader interviews support the assertion that as those with less experience may be overly optimistic in their organizations' ability to create consolidated action plans.

7. Comprehensive Resource Management

a. Quantitative Analysis

The Comprehensive Resource Management concept analysis in Table 10 only includes the Field group. There were no statistically significant results for the Command Structure group (*p* = .718). The Field group results are included for further analysis. The following survey questions were included, indicating both positive (+) and negative (-) versions:

> *+ My organization has a process when responding to cyber incidents to track resources from the initial request through their distribution and return, even when multiple organizations are involved.*
>
> *- There is no formal process in my organization to ensure that resources can be requested, allocated and tracked when responding to a cyber incident involving multiple stakeholders.*

Table 10. Resource Management Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	5.20	1.25				
Field	EM/HS IT/CS	48 31	5.25 5.15	1.32 1.14	1	-.36	.13	.718

Note: *95% Confidence interval used for calculating *p* values.

The results of the Field subcategory analysis as it relates to the Comprehensive Resource Management core concept indicate similar perceptions for both EM/HS and IT/

CS. With little difference in mean values, there is evidence to support both fields of discipline perceive an ability to implement comprehensive resource management principles during a significant cyber incident response. EM/HS and IT/CS respondents both somewhat agreed that their organizations are using these resource management concepts. Without further quantitative data to analyze, it is difficult to draw conclusions for this core concept.

b. Relevant Qualitative Findings

The qualitative findings for the Comprehensive Resource Management core concept indicate resource management is a concern and current capability for both EM/HS and IT/CS. This supports the quantitative results above. There appears to be consensus amongst the EM/HS leaders that ICS/NIMS is a good framework for resource management as it relates to assets outside of the technical human resources desired for a response. Resources such as food, beverages, sanitation, documentation, and other consequence management resources were all attributed to EM/HS personnel to organize. In a sign of maturing cyber incident response capacity, Director Willis described a local EM/HS organization providing resource management for both cyber and infrastructure/public health concerns during a recent cyber attack on a municipal water supply. He did go on to say that EM/HS do not have resource management for cyber resources fully developed yet. The technical human resources were specifically identified in four of the qualitative interviews as scarce resource during significant cyber incident response while that scarcity seemed implied in the remaining interviews.

The findings indicate that there is not a consensus regarding whether EM/HS or IT/CS would be responsible for filling the human resource needs. While all four EM/HS interviewees identified the role of providing the talent through EMAC and the activation of the National Guard, only two of the CISOs recognized that role during the interviews. One of the CISOs, David Allen, recognized the EMAC and National Guard resources and the tie to the EM/HS agencies but also noted that he considers one of the primary roles of his agency is that of a resource manager to get "the right resources to the right thing at the right time." Deputy CISO Swanson also brought up restrictions on incident response personnel due to cyber insurance policies that EM/HS professionals are likely not versed in. Another major challenge in cyber incident response was discussed by CISO Ford when he referenced problems communicating not only what resources are available but, more importantly, the true capabilities of those resources. There is doubt as to whether those in the EM/HS field have the in-depth understanding of cyber-security resources and capabilities to provide better resource management of cyber assets during response.

c. Summary

The results of the Field subgroup analysis were not statistically significant. The EM/HS and IT/CS fields of discipline rated their organizations' ability to provide comprehensive resource management virtually the same, resulting in inconclusive evidence to support any conclusions. The results may suggest that both fields of discipline have already developed some comprehensive resource management capability. Rating as only somewhat agree, the respondents indicate that there is still room for improvement in the application of the core concept. The qualitative findings support the results, with interviewees acknowledging challenges finding technical human resources to support cyber incident response. There was no consensus as to which field of discipline was better prepared to manage these technical cyber responders; however, the use of ICS/NIMS by EM/HS professionals was determined to be well suited for other resource management related to EMAC, National Guard Activation, food, sanitation, and consequence management.

8. Pre-designated Facilities

The analysis of the pre-designated Facilities concept is represented in Table 11. Only analysis of the Field group was included for further discussion, as no subgroups returned statistically significant results. There was only one question in the survey for this concept, the positive (+) indicator statement:

+ There is a pre-determined location for my organization to coordinate cyber incident response; including other organizations as necessary.

Table 11. Pre-Designated Facilities Descriptive Statistics and *ANOVA*

Element	Subgroup	*n*	*M*	*SD*	*df*	*t*	*F*	*p**
Sample		79	4.91	1.73				
Field	EM/HS IT/CS	48 31	4.73 5.19	1.92 1.38	1	1.17	1.36	.248

Note: *95% Confidence interval used for calculating *p* values.

The results of the quantitative analysis for the pre-designated facilities core concept indicate IT/CS organizations as having a higher (*M* = 5.19) ability and expectation to respond to a pre-designated location during a significant cyber incident than EM/HS organizations (*M* = 4.73). The total sample's mean (*M* = 4.91) was the third lowest overall, indicating a relatively low capability in this core concept compared to the other seven core concepts. The results do not provide robust evidence to support any conclusions; however, they may suggest that both fields of discipline somewhat agree that they have adopted the use of pre-designated facilities for incident response. Although the small difference in means indicates adoption of pre-designated facilities similarly across fields, IT/CS is slightly more likely to use these facilities in a significant cyber incident response.

a. Relevant Qualitative Findings

There are minimal qualitative findings for the pre-designated Facilities core concept. These findings do support the quantitative results indicating both EM/HS and IT/CS use pre-designated facilities as part of their response activities. The findings did identify differences in the two disciplines regarding use of pre-designated facilities for incident response. Director Phelps noted that facilities like a SEOC, commonly used by EM/HS for other disaster response, were a useful tool for coordinating concerns like consequence and resource management while also acknowledging that the IT/CS technical response would likely need to be near the impacted equipment or from an IT Security Operations Center

(SOC) where the technical response tools are available. This mirrors the lessons learned during the CDOT ransomware attack, according to Director Willis. Willis noted that pre-designated facilities were useful and he would encourage their use, but caveated that the non-technical aspects of response, such as logistics, the joint information center (JIC), and coordination with the federal government, were handled from the SEOC while the on the ground response occurred on site of the impacted network. This was important in the CDOT incident because having the responders in the same location allowed for the exchange of information in the absence of interoperable communications. In the case study he also revealed that pre-designated facilities could be weakness during a cyber response if employees all amass to a pre-designated location and plug in their laptops without knowing whether their laptops were infected. Willis also noted that during a pandemic having all responders come to a single location would not work. Conversely, CISO Ford noted that in a cyber response there would not necessarily be the need for pre-designated facilities. Ford went on to say that “a well-prepared organization can accept help from anywhere.”

b. Summary

The pre-designated facilities core concept did not have statistically significant results. There were also few qualitative findings in support or against the results. The EM/HS and IT/CS respondents both somewhat agreed that their organizations have adopted principles aligned with this core concept. What the results may suggest is that both groups have already established pre-designated facilities as part of their response plans, while the qualitative findings indicate that the location of the facilities differs by field of discipline. EM/HS participants referenced response efforts from a pre-designated SEOC while IT/CS responders were likely to work from a SOC.

9. Comparative Means Analysis

a. Quantitative Analysis

This section evaluates the eight core concepts by conducting an analysis of means test (ANOM). The means from each core concept are comparatively examined first by field of discipline, followed by previous experience in cyber incident response, length of time in field, career level, and finally type of organization. Then, the produced analysis is further evaluated using the ANOM function to compare each group mean to the overall mean looking for statistically significant results. A simple depiction of the means for each core concept sorted by field of discipline is in Table 12.

Table 12. Comparison of Core Concept Means by Field

Core Concept	EM/HS Mean	IT/CS Mean
Common Terminology	4.84	5.55
Integrated Communications	5.08	5.38
Modular Organization	5.24	5.13
Recognized Command Structure	5.65	5.31
Manageable Supervisory Structure	4.57	4.65
Consolidated Action Plans	4.92	4.87
Comprehensive Resource Mgt	5.25	5.15
Pre-Designated Facilities	4.73	5.19

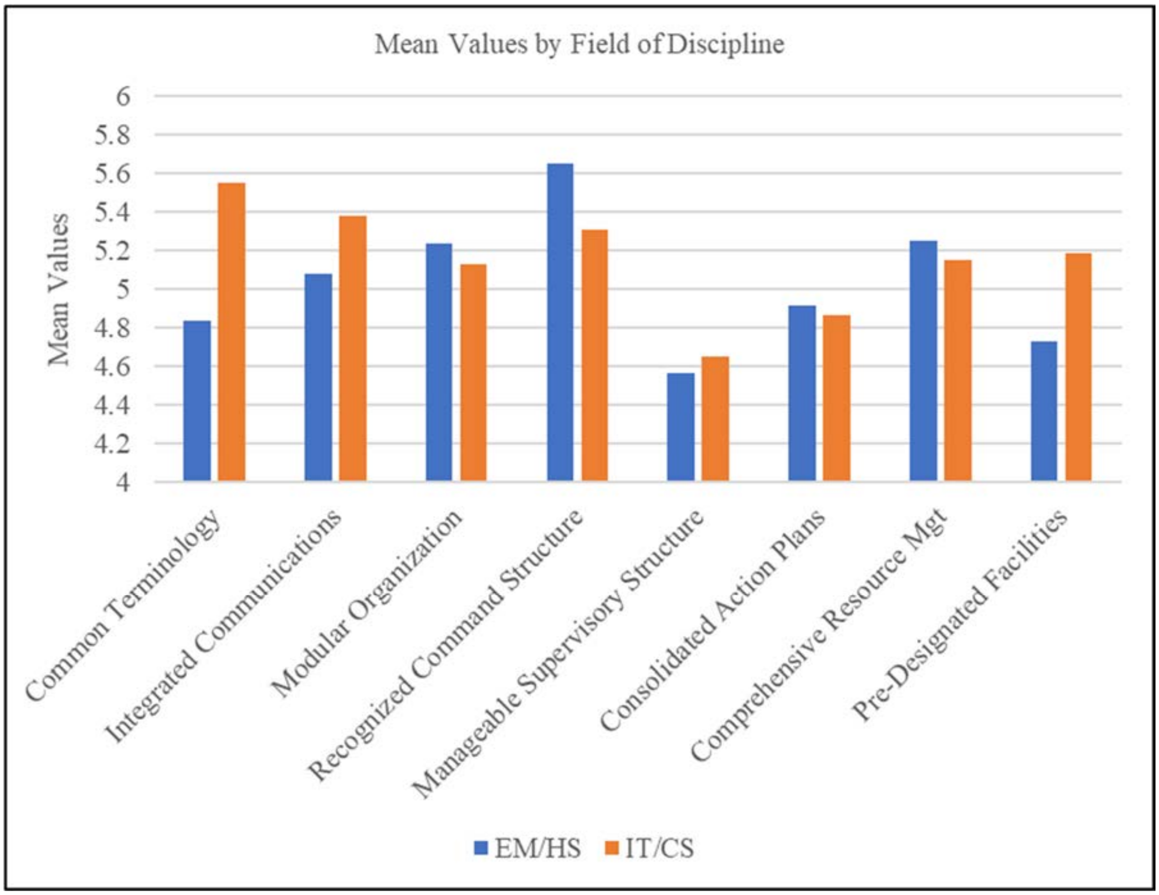


Figure 2. Comparison of Core Concept Means by Field

The EM/HS group rated their organizations' use of modular organization, recognized command structure, consolidated action plans, and comprehensive resource management higher than their IT/CS counterparts. The IT/CS group, meanwhile, rated their organizations' higher in the use of common terminology, integrated communications, manageable supervisory structure, and pre-designated facilities. There are multiple possible explanations for the variation in scores which is further evaluated later in this chapter. As a whole, however, the results suggest that each field's culture, training, and use of technology may impact their organizations' application of each core concept.

To better understand the mean values for each field, an evaluation of the correlations between each core concept's mean is useful. This can be done by calculating the Pearson correlation coefficient, which provides a numerical value to the correlations. To determine the Pearson's correlation coefficients, a multivariate analysis script was used in JMP Pro placing the means from each core concept on the Y axis. The results were then sorted by the field of discipline. The closer the coefficient is to 1 or -1, the stronger the correlation, with weaker correlations being closer to 0. Stated another way, the greater the number, the more likely a continued population sampling would produce similar results. Additionally, statistical significance was determined by running the correlation probability script within the program to calculate a *p*-value for each correlation. The following two tables include the Pearson's correlation coefficients and their relative *p*-values. Table 13 describes the results for EM/HS professionals while Table 14 represents the IT/CS results.

Table 13. EM/HS Pearson's Correlation Coefficients for Core Concepts

Measure	1	2	3	4	5	6	7	8
1. Common Terminology	–							
2. Integrated Communication	.69**	–						
3. Modular Organization	.54**	.68**	–					
4. Command Structure	.40**	.69**	.66**	–				
5. Span of Control	.39**	.70**	.45**	.43**	–			
6. Action Plans	.57**	.74**	.76**	.60**	.62**	–		
7. Resource Mgt	.43**	.65**	.76**	.61**	.62**	.76**	–	
8. Designated Facilities	.55**	.61**	.60**	.36*	.46**	.69**	.60**	–

Note. **p* < .05, ***p* < .01.

The results in Table 13 highlight the correlation of core concepts to each other based on the survey answers provided by EM/HS professionals. All results except one are statistically significant to the *p* <.01 level, with the lone outlier significant at *p* <.05. The results also indicate strong correlations (>.70) among action plans and integrated communications, action plans and modular organization, resource management and modular organization, and resource management and action plans.[146] Several other correlations nearly reached the level of "strong" correlation as well. Perhaps the most revealing result of this analysis, though, was the statistical significance across all core concepts. This seems to support a hypothesis that EM/HS professionals, who are assumed to have been trained in ICS, are responding or planning to respond to significant cyber events with some consistency relative to the eight core concepts. More simply put, the survey responses across core concepts were closely related to the responses to all of the other core concepts (correlation). Correlation does not necessarily equal causation, but in this evaluation, the results may be explained by the EM/HS group having training in ICS and/or past experiences implementing the framework (causation).

Table 14. IT/CS Pearson's Correlation Coefficients for Core Concepts

Measure	1	2	3	4	5	6	7	8
1. Common Terminology	–							
2. Integrated Communication	.44*	–						
3. Modular Organization	.54**	.53**	–					
4. Command Structure	.52**	.62**	.54**	–				
5. Span of Control	.16	.38*	.22	.23	–			
6. Action Plans	.11	.59**	.38*	.48**	.41*	–		
7. Resource Mgt	.12	.38*	.34	.40*	.70**	.65**	–	
8. Designated Facilities	.19	.49**	.24	.56**	.23	.06	.20	–

Note. *p < .05, **p < .01.

Table 14 represents the results of the multivariate analysis and *p* – value calculations for the IT/CS subgroup. Compared to the EM/HS results in Table 13, the IT/CS subgroup responses resulted in fewer statistically significant correlations as well as a

[146] Zach, "What Is Considered to Be a 'Strong' Correlation?," *Statology* (blog), January 22, 2020, https://www.statology.org/what-is-a-strong-correlation/.

lower degree of statistical significance where applicable. Of the 17 statistically significant results, six were at the *p* <.05 level, whereas the EM/HS group had 28 statistically significant results with only one being at the *p* <.05 level. This provides support for a lack of consistency in IT/CS response efforts as they relate to the eight core concepts of ICS. More notably, the Pearson's Correlation Coefficients of the eight concepts were lower in all instances but two (command structure / modular organization and resource management / span of control) for the IT/CS subgroup. In other words, the IT/CS group's responses were not strongly related across concepts (correlation), which indicates a higher degree of randomness between responses. A possible explanation for this lower connection between concepts is a lack of training and prior experience implementing the concepts as part of a systematic approach to response (causation). These results indicate evidence of consistency and overall greater application of the core concepts by EM/HS during significant cyber incident response.

b. Relevant Qualitative Findings

The quantitative results align with the qualitative research findings and literature. While ICS has been around since the 1970s and is the de facto standard due to federal grant requirements, cyber security as a field and cyber attacks as a threat requiring response is a developing field. Additionally, the federal government has developed full guidance and free training for ICS and NIMS through FEMA, which is required training for many EM/HS organizations for grant eligibility. In the interviews with the key leaders all four EM/HS leaders indicated that they would expect to integrate cyber security organizations into their ICS/NIMS structures, while acknowledging that the IT/CS organizations would not be as knowledgeable in the ICS/NIMS framework. Conversely, all four IT/CS leaders interviewed acknowledged an expectation that if the event became significant enough, they would have the ICS/NIMS framework "wrap around" their cyber response to ease the organizational burden on the technical cyber responders. As David Allen, CISO for the Georgia Technology Authority described it: "You let me handle the macro-level interagency stuff and we'll provide you top cover to dig into the technical details." In the case of Colorado, after responding to their CDOT incident, their cyber incident response plans are now being re-written to include ICS/NIMS terminology while also getting some of their key individuals trained in ICS/NIMS.

c. Summary

The comparative means analysis explored the average rating of each core concept by the EM/HS and IT/CS practitioners. The EM/HS subgroup rated their organizations higher in application of modular organization, recognized command structure, consolidated action plans, and comprehensive resource management, while the IT/CS subgroup rated their organizations higher in the use of common terminology, integrated communications and manageable supervisory structure. When analyzing the correlation of core concepts to each other and sorted by field of discipline, the results clearly showed that EM/HS practitioner responses were all correlated to each other in a statistically significant way. This suggests that the EM/HS subgroup’s training and experience using ICS has resulted in the core concepts being applied holistically as a system. Conversely, the IT/CS subgroup results revealed lower correlations as a whole, a result which indicates inconsistency of application of the eight core concepts systematically. The qualitative findings support higher levels of ICS/NIMS application, training and experience by EM/HS field. The findings also provide insight into the specific core concepts that IT/CS participants rated their organizations higher than their EM/HS counterparts, which are discussed further below in each core concept’s analysis section.

10. Summary

The results and supporting findings indicate that there are differences in the perception of organizational application of core concepts between EM/HS and IT/CS professionals. The results show that EM/HS responses were highly correlated across the eight core concepts, suggesting that their historical training and application of ICS in disaster response has resulted in consistency in application of the system; see Figure 3. Unsurprisingly, the IT/CS subgroup did not see the same level of correlation that would be expected from a group that has not been trained in ICS. In addition, while the EM/HS participants rated their organizations higher at implementing modular organization, recognized command structure, consolidated action plans, and comprehensive resource management; the IT/CS participants rated their organizations higher in the use of common terminology, integrated communications, manageable supervisory structure, and pre-designated facilities. The concepts that IT/CS responders are already rating themselves higher may be indicative of response functions that need less attention in a significant cyber incident. The core concepts that the EM/HS subgroup rated themselves higher in may then be viewed as areas of opportunity to provide increased assistance in similar response scenarios.

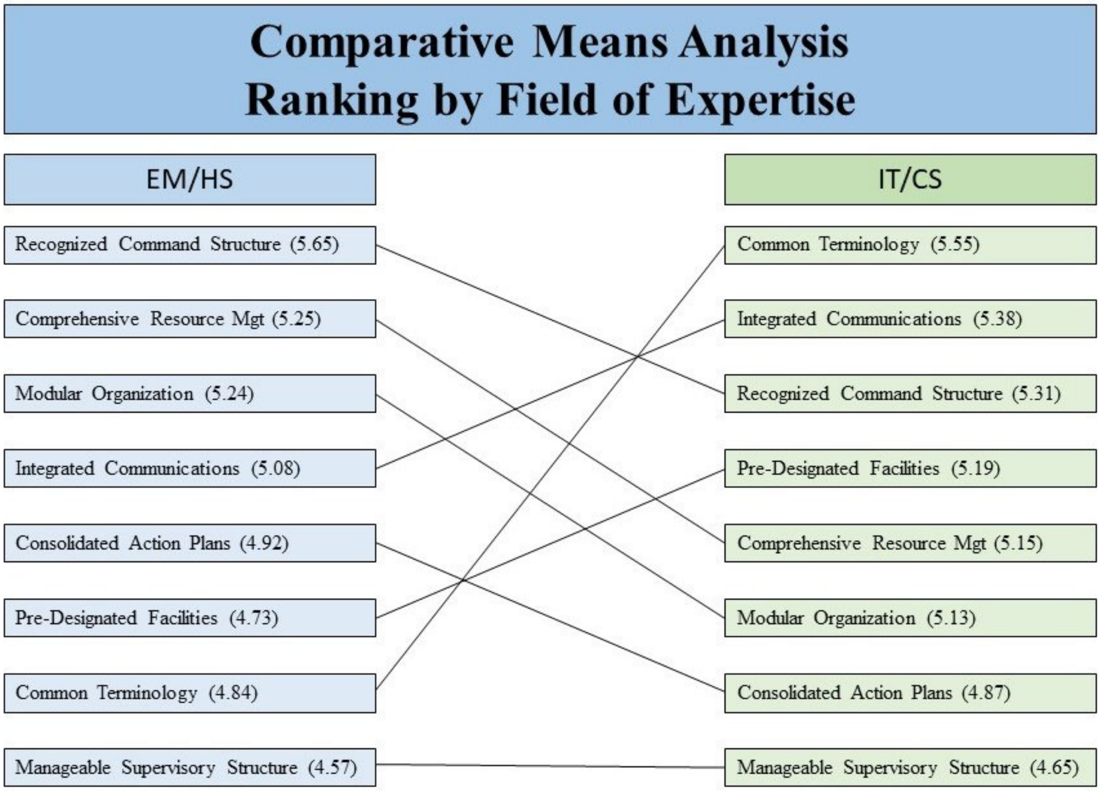

Comparative Means Analysis
Ranking by Field of Expertise
EM/HS
IT/CS
Recognized Command Structure (5.65)
Comprehensive Resource Mgt (5.25)
Modular Organization (5.24)
Integrated Communications (5.08)
Consolidated Action Plans (4.92)
Pre-Designated Facilities (4.73)
Common Terminology (4.84)
Manageable Supervisory Structure (4.57)
Common Terminology (5.55)
Integrated Communications (5.38)
Recognized Command Structure (5.31)
Pre-Designated Facilities (5.19)
Comprehensive Resource Mgt (5.15)
Modular Organization (5.13)
Consolidated Action Plans (4.87)
Manageable Supervisory Structure (4.65)

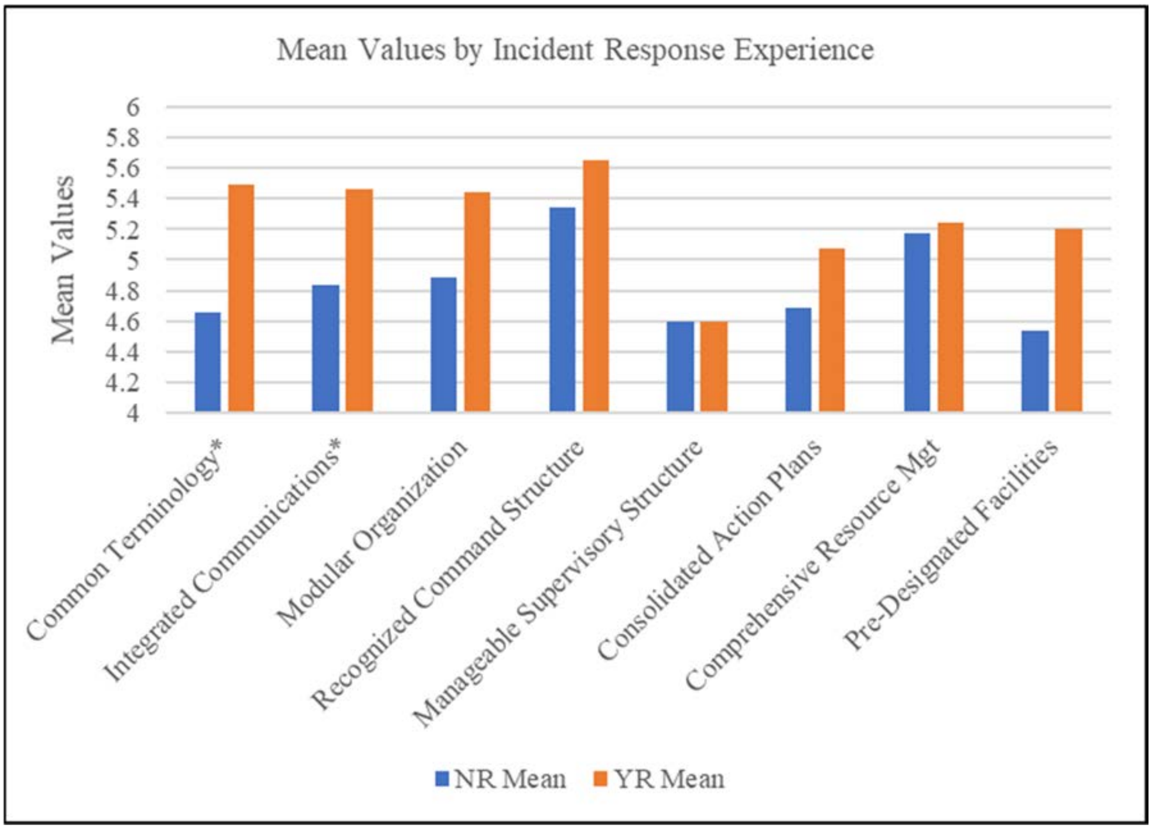
Figure 3. Ranking of Core Concepts by Field

Another conclusion that can be drawn from the results is that prior incident response experience raises the perception of core concept application. While only statistically significant for two core concepts, the pattern held across all concepts as shown in Table 15. The no prior incident response experience group (NR) and the prior incident response experience group (YR) did rate their the same after rounding for manageable supervisory structure; however, the YR group did rate their organizations slightly higher. This suggests that experiential learning from previous incident response can raise the perception of organizational competency in each of the concepts. The data does not state what framework was used during the prior incident response and includes both EM/HS and IT/CS survey responses. This makes it difficult to determine if the use of ICS during the responses was the reason for increases; however, due to the sample populations weight toward EM/HS participants, it can be assumed that the ICS framework was implemented in a significant amount of these incidents.

Table 15. Comparison of Core Concept Means by Response Experience

Core Concept	NR Mean	YR Mean
Common Terminology*	4.66	5.49
Integrated Communications*	4.84	5.46
Modular Organization	4.89	5.44
Recognized Command Structure	5.34	5.65
Manageable Supervisory Structure	4.60	4.60
Consolidated Action Plans	4.69	5.07
Comprehensive Resource Mgt	5.17	5.24
Pre-Designated Facilities	4.54	5.20

Note: *95% Confidence interval used for calculating *p* values.



Note: *95% Confidence interval used for calculating *p* values.

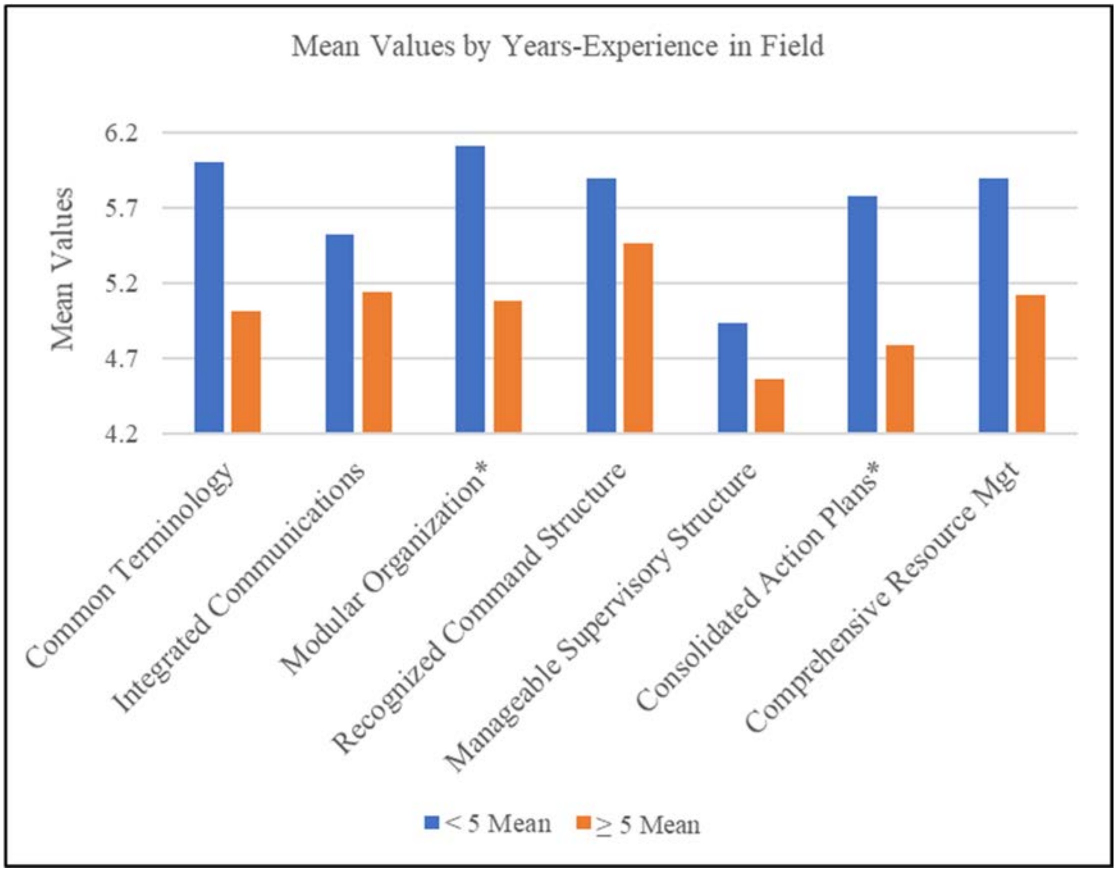
Figure 4. Comparison of Core Concept Means by Response Experience

The results also showed that those with less than five years of experience in their field rated their organizations higher across each core concept. This was statistically significant in three of the core concepts, but the pattern was true across all core concepts, adding further reliability. Table 16 shows the combined mean ratings of each core concept when sorted by years of experience in the field.

Table 16. Comparison of Core Concept Means by Years of Experience in Field

Core Concept*	< 5 Mean	≥ 5 Mean
Common Terminology	6.00	5.01
Integrated Communications	5.52	5.14
Modular Organization*	6.11	5.08
Recognized Command Structure	5.89	5.46
Manageable Supervisory Structure	4.94	4.56
Consolidated Action Plans*	5.78	4.79
Comprehensive Resource Mgt	5.89	5.12
Pre-Designated Facilities	5.67	4.81

Note: *95% Confidence interval used for calculating *p* values.



Note: *95% Confidence interval used for calculating *p* values.

Figure 5. Comparison of Core Concept Means by Years-Experience in Field

There were no findings to support or discredit these results as there are no specific questions related to the results in the semi-structured interviews. Based on the previous evidence supporting incident response experience as a factor that increases mean values for each core concept, and an assumption that less time in the field would correlate to less experience in significant cyber incident response, the time in field results may indicate that those with less time in their field simply "don't know what they don't know." Although there is no empirical research available on the matter, the SANS Institute previously published a paper by Charles Morris that recommended ICS be taught in Information Security training due to the lack of a standard crisis management model in the field.[147] This indicates a lack of training in incident response in programs that are producing new IT/CS professionals, which could partially explain the knowledge gap identified above. This may also be explained with an assumption that those practitioners in IT/CS and EM/HS are less likely to participate in meaningful ways during larger, multi-agency response exercises.

[147] Charles Morris, *Using the FEMA Incident Command System to Manage Computer Security Incidents* (Bethesda, MD: SANS Institute, 2004), 17–19, https://www.giac.org/paper/gsec/4037/fema-incident-command-system-manage-computer-security-incidents/106431.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The research has shown that the Incident Command System has been used successfully in significant cyber incident response. ICS has been adopted broadly across government and by first responders for disaster response, including the National Cyber Incident Response Plan.[148] As the de facto standard and "best bang for the buck" according to Hannestad, it has already been implemented in some of the early major response efforts as shown in the case studies.[149] Beyond examining its applicability, this thesis aimed to identify if ICS can improve significant cyber incident response, and if so; how. Quantitative and qualitative analysis of the eight core concepts of ICS indicated that some concepts are increasingly important in these cyber events while others are less applicable in cyber events than they are assumed to be in traditional disaster response. Additional results and findings have shown that experiential learning through cyber incident response increases the perception of implementation of the core concepts within an organization. Further, results identified an apparent over-estimation of the implementation of the core concepts by responders new to the field.

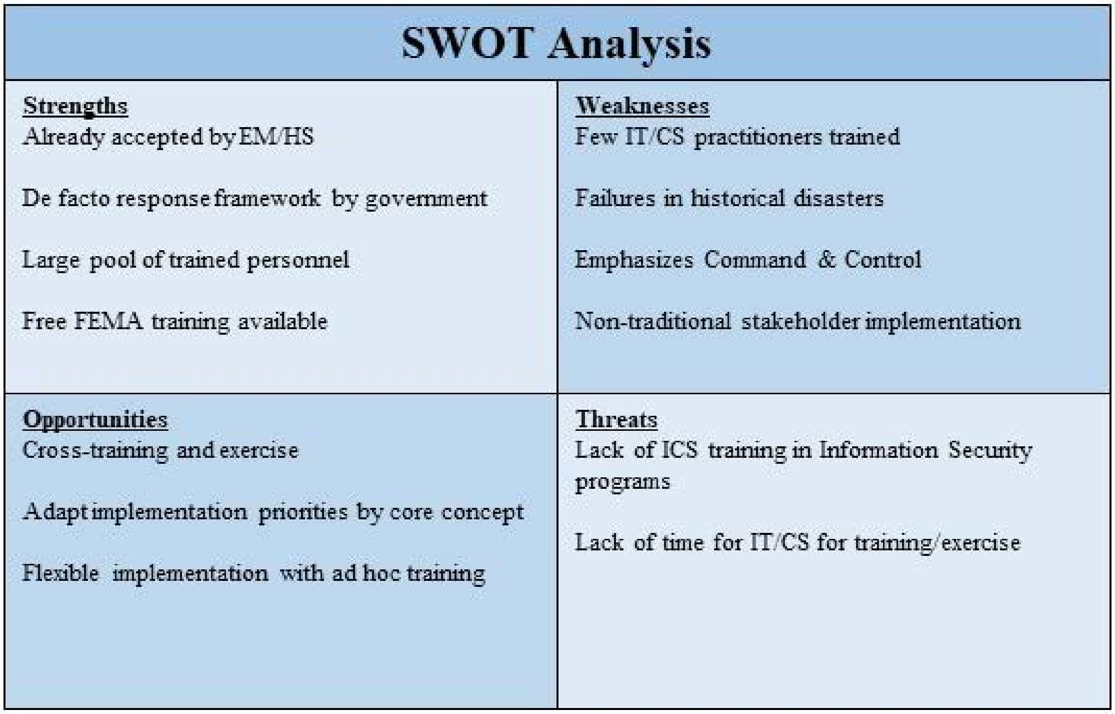
1. Apply Here

At the most basic level, this research aimed to determine if ICS was an applicable framework for responding to significant cyber incidents. The case studies and senior leader interviews supported the assertion that ICS was not only applicable, but also useful framework for these incidents. It should be noted, though, that the research did not attempt to apply ICS to more routine cyber emergencies. The findings did suggest that the framework would not be as applicable in these more routine emergencies. Specifically, in the CDOT incident, which was the first state declared cyber emergency, ICS was used effectively to better organize a response effort than the unstructured way the response was

[148] U.S. Department of Homeland Security, *National Cyber Incident Response Plan*, 8.

[149] Hannestad, "Developing National Standard," 26; and Harrald, "Agility and Discipline," 604.

being coordinated prior to the EM/HS arrival. Lessons learned from Colorado's experience have since been adopted in other significant cyber incident response efforts. Although the sample size is small thus far, ICS has shown value during cyber events. The case studies are further supported by findings from interviews with senior leaders in the EM/HS and IT/CS fields. A brief strength, weakness, opportunities, and threats (SWOT) analysis is provided in Figure 6 and the following paragraph.



SWOT Analysis

Strengths	**Weaknesses**
Already accepted by EM/HS De facto response framework by government Large pool of trained personnel Free FEMA training available	Few IT/CS practitioners trained Failures in historical disasters Emphasizes Command & Control Non-traditional stakeholder implementation
Opportunities	**Threats**
Cross-training and exercise Adapt implementation priorities by core concept Flexible implementation with ad hoc training	Lack of ICS training in Information Security programs Lack of time for IT/CS for training/exercise

Figure 6. SWOT Analysis

Some of the supporting factors for ICS are historical acceptance by the EM/HS practitioners, a wide range of personnel already trained in its use, free training available from FEMA, and broad applicability. On the other hand, ICS has shown weaknesses in evaluations of its implementation in large disasters, a perceived emphasis on command and control at the expense of collaboration, an inability to incorporate non-traditional stakeholders, and the fact that there are few IT/CS practitioners who are trained in the framework. There are opportunities to improve implementation of the framework in significant cyber incidents. For example, most of the leaders interviewed explicitly recommended cross-training between EM/HS and IT/CS as well as the need to conduct collaborative cyber incident exercises (see recommendations section below). Further, there are opportunities to use ICS's flexible nature to adapt the implementation based on an evaluation of the framework's core concepts (see subsection 2 below). One of the challenges to the adoption of ICS across significant cyber incidents is the lack of ICS training in Information Security programs and the focus on technical response actions. Another challenge, as indicated in the qualitative interviews, is the shortage of IT/CS practitioners who are already stretched thin within their organizations, a situation which makes allotting time for ICS training and exercises more difficult.

2. Improvement to the Core

The research provided insight into each of the eight core concepts of ICS which can be used to improve the framework's implementation in significant cyber incident response. The research also showed that EM/HS practitioners, who are assumed to have more ICS training and experience than their IT/CS counterparts, had higher correlation across all of the core concepts compared to the IT/CS practitioners. This higher degree of correlation may be interpreted as EM/HS showing more consistency in implementation of a framework that includes all eight core concepts. In addition, the research has shown that developing a common operating picture is a significant challenge, which has implications for certain core concepts.

The first core concept analyzed was the use of common terminology, where IT/CS practitioners rated their organizations better than EM/HS practitioners rated their own organizations. This may indicate that IT/CS as a field is better at applying the concept, providing opportunities to improve ICS if lessons can be learned from IT/CS frameworks or training. Conversely, it may just be attributable to the requirement by the IT/CS group to use specific, common terminology within their field as a necessary part of making information systems work. Still, the senior leaders interviewed recognized the inability of IT/CS and EM/HS fields to understand each other's terminology as a significant problem. This is important because an interviewee indicated that the EM/HS practitioners can become intimidated by the IT/CS practitioners in an emergency response, and this can reduce communication. The biggest problem in significant cyber incident response, according to the key leaders in this study, was the inability to develop a common operating picture quickly and accurately. Development of a common operating picture is key to any response effort because action plans and prioritization are based upon the information. An inability of the two fields to communicate effectively can be a significant hindrance when it is most important. Fortunately, the findings from at least one case study showed that the IT/CS responders were able to understand ICS processes after ad hoc training or explanation during the incident response.

The research also showed that the use of integrated communications is as important as using common terminology when coordinating a significant cyber incident response. Here again the IT/CS field rated their organizations higher than the EM/HS field. Integration of communications is essentially what enables computer networks to function and, therefore, may explain the IT/CS field's rating of the concept. Still, further research should consider what lessons may be learned from the IT/CS field's frameworks and processes related to integration of communications as way to improve ICS (see future research opportunities below). The research findings indicated that integration of communications was central to response leadership teams' ability to effectively communicate and develop the common operating picture. The Texas response also showed the concept's significance in coordinating response efforts across a large geographic space. The difference between the CDOT event and the Texas municipality attacks highlighted how having a central geographical location versus a geographically dispersed can change the importance of integrated communications. In an event where resources can be massed in one location, integrated technologies may be of lesser importance due to an ability to speak directly to the response team for the purposes of coordination. In the wake of the COVID-19 pandemic, though, there were senior leaders who indicated that planning to amass all the response personnel in one location may not be ideal. Therefore, one may conclude that there is an inverse relationship between the importance of integrated communications and the ability to congregate response personnel during an incident.

Although application of the modular organization concept was evident in the case studies, the research shows that the EM/HS field places a higher importance on the concept than IT/CS. This is an area where the ICS framework may better facilitate integration of non-traditional stakeholders by providing them structure to the command and control processes. For these reasons, modular organization may be considered a strength of ICS compared to the frameworks and processes that the IT/CS field uses.

The concept of recognized command structure again showed a difference in rating of application and ranking of concepts to indicate it as a strength of ICS. The EM/HS field rated higher their organizations' ability to apply the concept the highest of any concept in either group, while the IT/CS field rated the concept third. Findings related to the concept showed that there was a need for a command structure to set common strategies and objectives, while the EM/HS leaders interviewed still seemingly acknowledged that ICS may be the right framework despite its immaturity in significant cyber incident response. In short, someone or some group has to be in charge to set and implement a unified strategy, and the research indicates that right now ICS may be the best suited to organize that command structure.

The concept that both EM/HS and IT/CS research participants rated their organizations lowest in was manageable supervisory structure. While IT/CS rate themselves slightly higher than the EM/HS group for the concept, its overall importance may be lower in a significant cyber incident response. Conversely, the results may show that both EM/HS and IT/CS are using frameworks that are ineffective at ensuring manageable supervisory structure. The qualitative findings of the research suggest this may be due to the culture of the IT/CS field and the implementation of technology that enables a wider span of control for leadership. This is important because conflict could emerge within a command structure when IT/CS leaders look to spread the technical IT/CS human resources further than EM/HS leaders are accustomed. The EM/HS leaders can use this research to ensure flexibility of implementation of ICS and defer to the IT/CS leaders for the assignment of the technical human resources. In summarizing the manageable supervisory structure concept's applicability to significant cyber incident response, the research shows that the concept itself is either poorly implemented by the frameworks used by both fields in the study or it is not as important due to culture and technology. No significant results or findings suggest that ICS is or is not more useful than other frameworks for this concept.

The quantitative results of the research revealed that EM/HS rated their ability to apply the concept of consolidated action plans slightly higher than their IT/CS counterparts. Maybe more telling, was that the EM/HS group rated this concept fifth of the eight core concepts in application while the IT/CS rated it seventh. The qualitative interviews and case studies strongly supported the finding that consolidated actions plans were one of the most important concepts during significant cyber incident response. The reasoning for the importance of the concept according to the qualitative findings was the link to the resource management concept. The ability to better coordinate the action plans and assign resources is imperative in a cyber incident due to the lack of available cyber response resources, particularly, technical human cyber response assets. Based on the qualitative and quantitative findings, the research suggests that ICS can be used to improve significant cyber incident response relative to consolidated action plans when compared to the IT/CS frameworks used by the research participants.

As discussed above, the comprehensive resource management concept is important when bringing in additional response capabilities during significant cyber incidents. Similar to consolidated action plans, the EM/HS group rated their organizations' ability to apply the comprehensive resource management concept higher than did their IT/CS counterparts. While the difference in ratings between the two groups was not large, the comparative ranking for each field did indicate that the EM/HS group was better at applying the concept relative to the other concepts. The EM/HS group ranked the concept second compared to the IT/CS ranking of fifth. The qualitative findings suggested that one of the most important roles the EM/HS practitioners in a cyber incident response was the application of resource management. Most commonly, the senior leaders referred to the EM/HS group's role as managing resources specifically for the second and third order effects of a significant cyber incident while not clearly assigning that role for technical human response assets. This is likely due to the EM/HS group not possessing the understanding of information systems to get the right resources, to the right place, at the right time. EM/HS should then develop a better understanding of the IT/CS field and factors such as cyber insurance to better prepare for a significant cyber incident, which is further discussed in the recommendations section below. Overall, though, the research does indicate a clear use for the ICS concept of comprehensive resource management in significant cyber incident response while revealing room for improvement attainable by the EM/HS field learning more about the implications specific to a cyber response.

The last of the eight core concepts to be analyzed was the pre-designated facilities concept. The IT/CS field rated their organizations' adoption of pre-designated facilities higher than the EM/HS group while also ranking their adoption as the fourth highest of the concepts compared sixth by the EM/HS group. This is surprising, as virtually all EM/HS organizations have a version of an emergency operations center for multi-hazard response. The findings may explain this when looking at the two case studies in this research. Both case studies showed the value of SEOCs, but specific cyber incident locations are going to vary depending on who is attacked, when viewed from the EM/HS perspective. Technical cyber incident response will generally occur at the impacted location, for example, the impacted organization's server room, so EM/HS responders would not be able to have pre-identified response locations for cyber incidents while the IT/CS responders would know exactly where the response would occur. Going even further, in the Texas municipality case study, there were multiple response locations across the state, but one of the recommendations to come out of that event was to create a multi-hazard area near the SEOC as a pre-identified response coordination location. The case study did not discuss who, specifically, should create the multi-hazard area, but the context seemed to indicate a state agency. On the other hand, as shown in the CDOT case, the IT/CS responders can and likely do have pre-identified facilities they would go to for their own cyber incident response. Overall, the research supports the use of pre-designated facilities in two ways which are discussed here briefly, but more comprehensively in the recommendations section below. First, a SEOC should be used for logistics, response structure management, coordination with external partners, and other non-technical functions such as finance. Additionally, a central technical response coordination function should be established in a pre-identified facility. This function should be closely linked with the command and control center for overall incident coordination.

3. Prior Response Experience Matters

Possibly the most significant finding of the research is the impact of previous incident response on the quantitative results. The survey showed that survey participants who indicated at least one prior experience responding to a significant cyber event rated their organizations' higher in each of the eight core concepts of ICS. There is related research indicating the value of experiential learning in the EM/HS field, which further supports the importance of this study's results.[150] The finding also indicates that training, and possibly more importantly exercises, in responding to significant cyber incidents would be valuable. It should be noted, that while Director Willis credited prior joint cyber exercises with enabling their response during the CDOT incident, he was also critical of the lack of inclusion of ICS principles in those exercises. Establishing a baseline of response experience across an organization would thus be expected to raise organizational perception of core concept capabilities.

4. A New Known Unknown

An important finding of this research is the discovery that practitioners in both the EM/HS and IT/CS fields who have less than five years' experience over-estimate their organizations' implementation of the core concepts of ICS during significant cyber incident response. In other words, the less experienced simply "don't know what they don't know." This study attributes the knowledge gap to a lack of significant incident response experience, less experience working in multi-agency environments, an assumed lower involvement in joint cyber incident response exercises, and the lack of incident response training in Information Security training programs. The finding is significant due to the lack of technical cyber incident response personnel, which means that newer responders are likely to be involved in response situations where they are not prepared to work within

[150] Tiffany Danko, "Student Perceptions in Homeland Security and Emergency Management Education: Experiential Learning Survey," *Journal of Experiential Education* 42, no. 4 (2019): 1, https://doi.org/10.1177/1053825919873678.

their organizations' response framework during a multi-agency cyber incident response. Ideally, all respondents would rate perceptions of their organizations highly in each core concept with corresponding results after an incident. However, the identification of the differences in perception can at least be used to focus limited resources to close the perception gap across experience levels.

B. RECOMMENDATIONS FOR ADAPTING AND ADOPTING ICS DURING CYBER INCIDENTS

1. Implement ICS in Significant Cyber Incident Response

The first and most basic recommendation is for government agencies to codify ICS as the response framework for significant cyber incidents. Government and other traditional responders are already using the framework for other disasters, so officially adopting ICS in these cyber incidents would provide continuity across disciplines. To make the implementation official, EM/HS practitioners should add cyber incident response annexes that include ICS/NIMS terminology to existing operations plans. Similarly, IT/CS practitioners should adopt ICS/NIMS terminology and concepts within their cyber incident response plans. As previously noted, the research did not indicate that ICS is applicable to more routine cyber incidents. Therefore, pre-identified triggers for implementation of ICS should be established such as a governor's emergency declaration or when critical infrastructure services are disrupted. Implementation of ICS in cyber incident response plans would not be without challenges. Re-writing or creating new incident response plans is time consuming and may be a low priority for already understaffed IT/CS personnel. Further, the implementation of ICS will require buy-in from key leaders who may already have invested efforts into establishing other response frameworks or who simply do not see ICS as applicable beyond natural hazards. Finally, although the case studies show that EM/HS can implement ICS by conducting ad hoc training during an event or wrapping the framework around the technical cyber response, it is assumed that providing training and exercise in the use of ICS during significant cyber incidents would be more effective but require more time and resources.

2. Include Cross Training and Collaborative Exercise

Providing cross training and collaborative exercise opportunities between EM/HS and IT/CS practitioners will increase the effectiveness of significant cyber incident response. Virtually all senior leaders interviewed recommended cross training between the two disciplines and the case studies both suggested ICS training as well. EM/HS practitioners should obtain basic cybersecurity training to better understand terminology used in the IT/CS field as well as what IT/CS responders do during cyber incident response. This will help the emergency management field normalize cyber incident response in a disaster management context. Conversely, IT/CS practitioners should seek training on basic ICS courses, such as those provided by FEMA's independent study courses and the Emergency Management Institute. The quantitative results also supported ICS training as a factor that increases the correlation of the core concepts of ICS. IT/CS practitioners would not need to become experts in ICS, but rather would be more able to understand the response framework construct under which they would be operating during a significant cyber incident. An additional expected benefit of cross-training is an increased ability to develop a common operating picture.

To build on the cross training, participation in significant cyber incident response exercises would be beneficial. The research consistently showed that those with previous cyber incident response experience rated their organizations higher in their implementation each of the eight core concepts of ICS. It would be impractical and ill-advised for an organization to wait for a significant cyber incident to build future response capability; therefore, the best substitute for this experience is participation in exercises designed to replicate significant cyber incidents. Senior leaders interviewed recommended enhancing collaborative exercises by having actual networked systems impacted to test technical cyber skills while also integrating EM/HS participants and ICS. A note of caution on these exercises: they should not be simply ICS exercises that are initiated by a notional cyber event, but rather should include a technical response component.

A key consideration for implementing training and exercises for significant cyber incidents is the involvement of practitioners in both fields who are earlier in their careers. The results of the study showed that practitioners in both fields were more likely to overestimate their organizations' ability to implement the core concepts of ICS. The results conflicted with their more experienced peers and the EM/HS field, who are assumed to be more knowledgeable and experienced in large, multi-stakeholder response efforts. This outcome was simply described in this research as the less experienced not knowing what they don't know. In order to better prepare for a significant cyber incident response, training and exercise coordinators should make a concerted effort to include those new to their fields, regardless of whether they are an EM/HS or IT/CS practitioner. One researcher also recommends that ICS training be included as part of the standard training for Information Security programs, which would be particularly valuable for Cyber Incident Response Teams.[151]

Adding training and exercises while also changing already developed training is not likely to go unchallenged. One of the biggest barriers to overcome may be the need to spend valuable training resources on ICS training rather than the technical information technology training that is ever-changing. As technologies change, IT/CS practitioners are necessarily tasked with learning and implementing the newest technologies. Similarly, it may be unreasonable to expect EM/HS to keep up with the new technologies, systems and threats, even at the most basic level. Further complicating the efforts are the potential for technical experts to be wary of systems that were developed by outsiders to their field.

3. Focus on Common Operating Picture

Developing a common operating picture was a common challenge across case studies and the qualitative interviews. In order to provide better significant cyber incident response; training, exercise, and real-time response activities should focus on developing a common operating picture. This can be accomplished through improved application of the core concepts of common terminology, integrated communications, and recognized command structure. If automation is the most efficient form of completing a task, North Dakota CISO Kevin Ford described the efficiency of IT systems in such a way that it may be applied to cyber incident response with human responders. Ford stated that you should

[151] Morris, Using the FEMA Incident Command System, 19.

first pre-negotiate and from there, as long as everyone is speaking the same language on the same platforms, you can automate. While humans cannot be automated, this can be applied to the human element of cyber incident response by first pre-negotiating as much as possible. EM/HS and IT/CS leaders should pre-negotiate and identify in their plans who will be initially responsible for assessing the cyber impacts and who will be responsible for assessing second and third order effects (recognized command structure). Pre-negotiation should also include what platforms, protocols and participants will be part of a response in a communications plan (integrated communications). Increasing the use of common terminology can be realized through the previously discussed recommendation of training and exercise and/or the creation of a Unified Command that includes members who can translate between the EM/HS and IT/CS disciplines. By pre-negotiating tasks and communications plans while ensuring common terminology, developing a common operating picture can be completed faster with more robust information that can be used to establish unified strategies, priorities and plans of action.

Challenges to the specific tasks within this broader recommendation are likely. One challenge discussed in the case studies was the desire to restrict information to protect criminal cases and law enforcement sensitive information. Another important challenge is the culture of secrecy surrounding cyber incidents which results in initial reporting being delayed as discussed by CISO Allen of Georgia. Finally, external stakeholders who have not participated in the pre-negotiating process may either be unwilling or unable to interact with the Unified Command.

4. Integrate Communications and Pre-plan for Multiple Response Locations

Both case studies revealed strengths and weaknesses of pre-designated facilities in cyber incidents. Colorado and Texas used their state emergency operations centers to coordinate response the non-technical response efforts such as logistics, finance, and resource recruitment. Meanwhile, Colorado indicated a key factor to their response success was the use of the Department Operations Center (DOC). Texas, on the other hand, noted that there should be a pre-identified and known multi-hazard event location specifically for the cyber responders. The technical on scene cyber incident response, though, will almost assuredly be at the location where IT networks are impacted. The network locations should therefore pre-plan to receive response assets and to coordinate with an off-site command and control group. This pre-planning should include simple logistic considerations such as adequate workspace for an expanding response team, sufficient network connectivity, ample electricity, locations for sustenance, and bathrooms. The central command and control location, such as the SEOCs used in Colorado and Texas, should focus efforts and pre-planning on the management of second and third order effects. One of the key functions of the central command and control location, according to CISO David Allen, should be to provide top cover for the limited technical cyber resources.

To facilitate response efforts across these multiple locations, both the central command and control site and on the local network locations should focus on increasing integrated communication capabilities. The first consideration should be to provide known communications platforms and protocols. A national, regional, or statewide standard for platform and protocols could ensure broader access to remote response assets as well as allow for quicker integration of external response resources. A second, and important consideration for integrating communications, is the need to pre-plan separate redundant communication systems. As recognized in both case studies in this thesis, the communications systems and networks at the primary response locations were impacted by the cyber event. This led to the need for communications across secondary channels to coordinate response for those who were not at the response site. Further increasing this importance is the potential for the pre-designated facilities to be impacted by the significant cyber incident. A higher degree of communications can also facilitate a larger span of control amongst the IT/CS responders.

There are challenges to preparing pre-identified response facilities and integrating communications in significant cyber events. A pandemic such as COVID-19 decreases the ability for response leadership to centralize response assets in pre-designated facilities and thus, increasing the importance of integrated communications. While preparing a command and control center in one location such as a SEOC is relatively easy, preparing and pre-identifying a response facility everywhere that could potentially be the victim of a cyber attack is unlikely to occur. It would also be difficult to get buy-in and agreement on specific communications platforms and protocols considering the diversity across government, the private sector, and non-government organizations. There will also be difficulty determining which systems will be adopted, those used primarily by EM/HS practitioners or those used in the IT/CS field. This challenge may be mitigated by the adoption of EM/HS tools, such as WebEOC, for the incident management platform relative to second and third order effects and resource tracking while adopting communication and collaboration tools specific to the IT/CS field. A final, common hurdle will be the allocation of resources to develop the plans and procedures and proceeding acquisition of technology.

5. Comprehensive IT/CS Human Resource Management

The final recommendations center around the scarcity of technical IT/CS human response resources. The central command and control organization should develop a comprehensive list of potential IT/CS response assets. To increase the value of this list, it should be developed in a standardized format based on a national criterion such as FEMA's resource typing to enable broader distribution of resource requests and timelier fulfillment. As noted by CISO Ford in his interview, it is also imperative to ensure an accurate understanding of each response assets true capability. To facilitate this accurate understanding, EM/HS and IT/CS leaders should collaborate on the development and maintenance of any such list. IT/CS training for EM/HS personnel would also assist in the development of resource lists. A second human resource management recommendation is maximizing the ability of IT/CS response resources to focus on technical response activities. To achieve this, EM/HS at the command level should continually evaluate action plans for opportunities to assign the non-technical response personnel to tasks that do not require the IT/CS skillset, therefore freeing IT/CS practitioners to complete their work. A final IT/CS human resource management issue is the need for EM/HS leadership to better understand the broader context of cyber incidents and the IT/CS operating environment. An example of the need to understand the broader context is the implications of cyber-insurance. As Deputy CISO Swanson points out, cyber-insurance policies may require specific response assets be deployed and limit other response assets. All of these technical human resource recommendations would aid in maximizing a severely limited resource.

Barriers to implementing these recommendations are significant, but not insurmountable. Development of a comprehensive resource list will be difficult without significant guidance at the national level from FEMA, DHS, or NIST, for example. While FEMA has begun some resource typing for cyber incidents, it is not comprehensive and, as Director Willis points out, "We're not there yet with cyber." The second component of these recommendations is IT/CS training for EM/HS personnel. Participating in sufficient training to understand an entirely different field requires immense resources and time, only to have the technologies changing at an exponential rate. This impacts the command and control unit's ability to request the right resources, assign resources in the most effective way, and to understand the context of a significant cyber incident's operating environment. While there is no expectation for EM/HS to become IT/CS experts, even the achievement of developing an appropriate baseline will be a challenge.

C. FUTURE RESEARCH OPPORTUNITIES

This thesis is narrowly focused on ICS for responding to a significant cyber incident and is heavily reliant on state level leadership for qualitative findings. It is further limited by few cases for review and the constantly changing cyber threat landscape. There are several areas of future research that should be undertaken.

1. Crisis Management Frameworks

ICS is currently the de facto standard for disaster management by emergency management professionals and is the identified framework for responding to significant cyber incidents in the National Cyber Incident Response Plan (NCIRP).[152] One of the weaknesses of this research is its sole focus on ICS as a means of scoping the effort. The research did not indicate that IT/CS professionals have implemented ICS in their operations to great extent, nor have they embraced it universally as a response framework for significant cyber incident response. For this reason, other known crisis management frameworks, particularly any identified by IT/CS professionals, should be evaluated for

[152] Harrald, "Agility and Discipline," 263; and U.S. Department of Homeland Security, *National Cyber Incident Response Plan*, 8.

their applicability to organize a response to significant cyber incidents. Further evaluation of crisis management frameworks that have been used in events similar to those in the case studies could provide lessons to improve ICS as long as it remains the de facto standard or replace ICS for significant cyber incident response.

2. Recovery

The NCIRP recognizes NIMS as the common incident management structure to recover from a significant cyber attack.[153] The case studies examined did not differentiate the response from recovery phases in the available materials; however, recovery of systems may last considerably longer than initial response to an incident. A weakness of this study was its narrow focus on response without consideration for other phases of emergency management. Research into the application of ICS specifically during the recovery phase would benefit implementation and operation of ICS more holistically.

3. Adaptation to Routine Cyber Incidents

Most cyber attacks do not meet the definition of significant cyber incident as studied in this thesis. A weakness of this research is that it focused on the larger, less frequent variations of cyber attacks. Further, it is not clear that all participants in the qualitative and quantitative research had a universal understanding of the terms significant cyber incident. Application of ICS in smaller, more routine cyber emergencies could be beneficial to organize the response structure but may require tailoring the concepts to better fit the operational environment of cyber security operations centers. Research into the way ICS would function in smaller-scale events and how ICS could be adapted may improve cyber incident response as a discipline.

4. Expansion of Stakeholders

In the United States, the private sector owns and operates most of the critical infrastructure; yet, this study did not involve private sector critical infrastructure

[153] U.S. Department of Homeland Security, *National Cyber Incident Response Plan*, 9.

stakeholders in either case study or in the qualitative interviews.[154] While there was some quantitative data collected specific to critical infrastructure, the limited survey sample size and lack of private sector senior leader interviews are weaknesses of this study. With nation-states showing a willingness to attack a critical infrastructure such as a power grid, ensuring a common approach with private sector stakeholders seems imperative.[155] A specifically designed study to evaluate the use of ICS to respond to significant cyber incidents in a private sector environment would validate or dispute the conclusions of this study.

[154] U.S. Department of Homeland Security, 10.

[155] Laurens Cerulus, "How Ukraine Became a Test Bed for Cyberweaponry," Politico, February 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: QUALITATIVE INTERVIEW QUESTIONS

Semi-Structured Leadership Survey		
	Emergency Management / Homeland Security	**Information Technology / Cybersecurity**
1	Have you been provided and agreed to the informed consent agreement?	
2	Can you describe any experience you have responding to significant cyber incidents, or what your expectations of the incident would be if you haven't been a part of one so far?	
3	What would you consider to be the biggest challenge in responding to a significant cyber incident?	
4	How would you compare responding to significant cyber incidents and more traditional "disasters" such as floods, hurricanes, or wildfires?	
5	In the event of a significant cyber incident, what framework would your organization use to organize the response and why?	
6	Can you expand on any strengths of your chosen framework and how they relate to multi-agency coordination?	
7	What would you consider some of the biggest weaknesses of your response framework?	
8	Based on your knowledge of the Incident Command System and the National Incident Management System, what are the reasons you think ICS/NIMS is or is not a good framework for significant cyber incident response?	How familiar are you with the Incident Command System and the National Incident Command System? A) If familiar - What are the reasons you think ICS/NIMS is or is not a good framework for significant cyber incident response B) If not familiar - What do you think are the most important qualities of any response framework during significant cyber incidents.
9	If you could give advice to IT/Cybersecurity leadership about preparing to work with your organization during a significant cyber incident, what would it be?	If you could give advice to Emergency Management/Homeland Security leadership about preparing to work with your organization during a significant cyber incident, what would it be?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: SURVEY QUESTIONS

Significant Cyber Incident Response Organization Survey

Section 1: Demographics

1	The field of discipline that most closely resembles my current position is:		
	○	Emergency Management / Homeland Security	
	○	Information Technology / Cybersecurity	
	○	Other:	*Briefly describe your field of discipline here*
2	My position within my organization is best described as:		
	○	Practitioner	
	○	Mid-Management	
	○	Senior Leadership	
3	My length of experience in my profession is:		
	○	Less than 5 years	
	○	5-10 years	
	○	More than 10 years	
4	My organization can best be categorized as:		
	○	Local Government	
	○	State Government	
	○	Federal Government	
	○	Private Sector Critical Infrastructure	
	○	Private Sector Non-Critical Infrastructure	
	○	Other:	*Briefly describe your organization's category here*

5	In my career I have:		
	○	Never been involved in a significant cyber incident response	
	○	Been involved in a significant cyber incident response once	
	○	Been involved in multiple significant cyber incident response efforts	
6	Regarding my organization, to my knowledge:		
	○	Has never been involved in a significant cyber incident response	
	○	Has been involved in a significant cyber incident response once	
	○	Has been involved in multiple significant cyber incident response efforts	
7	In my organization, during a significant cyber incident response we have used or plan to use:		
	○	National Institute of Standards & Technology (NIST) Cybersecurity Framework	
	○	Incident Command System / National Incident Management System	
	○	Both	
	○	Other:	*Briefly describe the response framework or incident management system*

8	I am familiar with the National Institute of Standards & Technology (NIST) Cybersecurity Framework						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
9	I am familiar with the Incident Command System (ICS) / National Incident Management System (NIMS)						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

Section 2: Incident Management Core Concepts							
10	My organization uses common terminology during significant cyber incident response that is easily understood by outside agencies.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
11	My organization does not use a common communications plan, interoperable communications processes, or interoperable systems during significant cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
12	During a significant cyber incident response, my organization takes a modular approach that allows it to expand to include additional internal and external stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
13	There is no plan or policy in my organization to ensure that supervisors maintain a manageable number of subordinates during incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

14	During incident response, my organization’s processes are designed to incorporate multiple organizations in the adoption of goals, strategies and action plans to minimize duplication of efforts.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
15	My organization does not have an existing plan to ensure common systems and processes for communications are in place with external and internal stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
16	There is no formal process in my organization to ensure that resources can be requested, allocated and tracked when responding to a cyber incident involving multiple stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
17	My organization’s incident response framework is not designed to incorporate other external stakeholder leadership in a unified command approach.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

18	There is a pre-determined location for my organization to coordinate cyber incident response; including other organizations as necessary.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
19	When responding to a significant cyber incident involving multiple organizations, there is no formal mechanism in my organization to ensure a unified set of strategies, objectives and goals is incorporated.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
20	As a general rule, my organization has procedures in place to ensure supervisors do not have more subordinates than they can manage during a significant cyber incident.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
21	My organization has a process when responding to cyber incidents to track resources from the initial request through their distribution and return, even when multiple organizations are involved.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

22	My organization uses a common communications plan that has interoperable processes and systems for coordinating with external agencies during significant cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
23	During a cyber incident response my organization collaborates with other agencies to create a single, formal document stating incident goals, objectives, and strategies.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
24	My organizations structure is not designed to expand or contract based on the complexity when responding to a significant cyber incident.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
25	Common terminology that is easily understood by external organizations is not used by my organization during a significant cyber incident response						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

Section 3: Incident Management Core Concepts - External Organizations							
26	Other organizations inside and outside of my profession use similar language for resources, organization functions, and facilities as mine during cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
27	External stakeholders that my organization may work with during cyber incident response do not have communications technologies and processes that are readily integrated into response efforts.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
28	Other organizations are prepared to scale their response organizations up or down depending on the complexity of the incident.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
29	Incorporating multiple stakeholder group leaders during cyber incident response into one unified command to form objectives and strategies is not a strength of organizations I work with.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

30	Other organizations seem to have supervisors who are able to maintain effectiveness because of their span of control during significant cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
31	A general weakness of external organizations during a cyber incident response is a lack of single, formal plan of action that has been coordinated with all stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
32	During incident response, I believe that other organizations have comprehensive resource management strategies that ensure the right resources get to the right places at the right time.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
33	Other organizations do not have pre-designated facilities where response functions can take place during a significant cyber incident.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

34	During significant cyber incident response, other organizations do not use terminology that is easily understood by multiple stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
35	During significant cyber incident response, partner organizations are setup with communications systems that integrate with my organization and others.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
36	The stakeholders my agency works with do not easily incorporate internal and external partners to increase response capacity as a significant cyber incident unfolds.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
37	When responding to a significant cyber incident, other organizations closely work together to form a unified response with shared objectives, strategies and resources.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

38	It is not uncommon for other organizations to have supervisors struggle with oversight due to having too many subordinates during cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
39	Other organizations tend to be effective because they have a well-defined, formal incident action plan stating common goals, objectives and strategies derived from collaboration with stakeholders.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
40	A common problem other organizations have is a lack of structured resource management systems for identifying, requesting and tracking resources during a cyber incident response.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○
41	External organizations that I am familiar with have facilities identified in advance to house critical incident response operations.						
	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
	○	○	○	○	○	○	○

APPENDIX C: SURVEY DATA

Response ID	Field of Discipline	Org Position	Experience	Org	Incident Experience	Org Response Framework	NIST Familiarity	ICS/NIMS Familiarity	Common Terminology (AVG)	Integrated Comms (AVG)	Modular Org (AVG)	Command (AVG)	Span Control (AVG)
1	EM/HS	SL	≥5 yrs	GO	YR	Other	Yes	Yes	6	4.67	6	6.5	3.5
2	EM/HS	MM	≥5 yrs	GO	No	ICS/NIMS	Yes	Yes	4	6.33	7	6.5	5
3	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	6.5	6.00	6.5	6.5	4
4	EM/HS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	6.5	5.33	7	6	6
5	EM/HS	PR	≥5 yrs	GO	YR	Both	Yes	Yes	6.5	7.00	7	7	7
6	EM/HS	SL	≥5 yrs	PS	YR	Both	Yes	Yes	6	6.00	6	6	4
7	EM/HS	MM	≥5 yrs	GO	YR	ICS/NIMS	Yes	Yes	3	3.33	5	5.5	2
8	EM/HS	SL	<5 yrs	GO	No	Both	Yes	Yes	5	2.67	5	2.5	2
9	IT/CS	SL	≥5 yrs	GO	No	NIST	Yes	Yes	4	4.67	2.5	2.5	4
10	EM/HS	SL	≥5 yrs	GO	YR	Both	Yes	Yes	6.5	6.00	6.5	6	4
11	IT/CS	MM	≥5 yrs	GO	YR	NIST	Yes	No	7	5.00	6	5.5	2.5
12	IT/CS	SL	≥5 yrs	PS	YR	Both	Yes	Yes	6	5.33	5.5	3.5	6
13	IT/CS	PR	<5 yrs	GO	YR	Both	Yes	Yes	7	7.00	7	6.5	6
14	IT/CS	SL	≥5 yrs	GO	YR	Both	Yes	Yes	6	6.00	6.5	6.5	6
15	IT/CS	PR	≥5 yrs	GO	YR	Both	Yes	Yes	6.5	4.67	5.5	5	4
16	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	4.5	4.67	5.5	6	2
17	EM/HS	PR	≥5 yrs	OT	YR	Both	Yes	Yes	4.5	4.67	6.5	5	4.5
18	EM/HS	PR	≥5 yrs	GO	No	ICS/NIMS	Yes	Yes	5	5.00	1.5	6.5	4.5
19	EM/HS	SL	≥5 yrs	GO	No	Unknown	No	Yes	2.5	3.33	3.5	6	2.5
20	IT/CS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	6.5	6.67	4	6.5	5.5
21	EM/HS	SL	≥5 yrs	GO	No	Both	No	Yes	4	4.33	6.5	6.5	3.5
22	IT/CS	SL	≥5 yrs	GO	YR	Both	Yes	Yes	6	6.00	6	5	4.5
23	IT/CS	SL	≥5 yrs	PS	No	NIST	Yes	Yes	6	4.33	4	6.5	3
24	EM/HS	MM	≥5 yrs	GO	YR	NIST	Yes	Yes	3	4.67	4	5.5	3
25	EM/HS	SL	≥5 yrs	PS	YR	ICS/NIMS	Yes	Yes	6.5	7.00	7	7	6.5
26	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	5.5	6.00	6	6	4.5
27	EM/HS	MM	≥5 yrs	OT	No	NIST	No	Yes	4	4.00	4	5.5	4
28	EM/HS	SL	≥5 yrs	GO	No	Both	No	Yes	5.5	3.67	4.5	5	4
29	EM/HS	SL	≥5 yrs	GO	No	Both	No	Yes	6	4.67	6	6	5.5
30	EM/HS	PR	≥5 yrs	GO	No	ICS/NIMS	No	No	4	2.67	2.5	3.5	1.5
31	OT	SL	<5 yrs	GO	No	ICS/NIMS	No	Yes	6.5	5.67	6	5.5	5.5
32	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	3.5	4.67	4	6.5	3

Response ID	Action Plans (AVG)	Resources (AVG)	Facilities (AVG)	Ext Common Terminology (AVG)	Ext Integrated Comms (AVG)	Ext Modular Org (AVG)	Ext Command (AVG)	Ext Span (AVG)	Ext Action Plans (AVG)	Ext Resources (AVG)	Ext Facilities (AVG)
1	6	6	6	4	3.5	4	4	1	4.5	4	4
2	6	6.5	4	3.5	4	4.5	3.5	3	4	3.5	1.5
3	5.5	7	6	6	6	6	6	4.5	4	5.5	5
4	5	5.5	7	5.5	6	6.5	5.5	4	4	4.5	4
5	6	7	7	7	7	7	7	5	6	5.5	6.5
6	6.5	6	7	6	6	6	6	5	6	6	6
7	4.5	5	3	4	3.5	3.5	4	5	4.5	2	4.5
8	4	4	2	4	4	4	4	4	4	4	4
9	6	5.5	2	5	4.5	4.5	5	3	3	4	4
10	6	6	6	6	6	6	6	5.5	4	6	6
11	4	4.5	6	6	6	6.5	6	3	5	6	6
12	2	3.5	6	5.5	6	6	5.5	5.5	4.5	5.5	6
13	7	7	6	6.5	5.5	6	6.5	3	2.5	2.5	3.5
14	6	6.5	6	4	5	5.5	4	4	5	2.5	2.5
15	4	4.5	5	5	4.5	4.5	5	4	3.5	4	4
16	4.5	3.5	3	3	4	4	3	3.5	2.5	3	3
17	5	4	4	5	4	5.5	5	4	4	4.5	4.5
18	4	2.5	2	4.5	4.5	5	4.5	5.5	3.5	4	5
19	2.5	2.5	2	4	4	4.5	4	4	3.5	4	4
20	5.5	5.5	6	4	4	4	4	3.5	3	4	4
21	6.5	7	6	3	4	5.5	3	4	2.5	3.5	3.5
22	6.5	5	3	6	6	5	6	5	5	3.5	4.5
23	3	4	6	5	4	4	5	4	4	4.5	4.5
24	4.5	5	3	3.5	4	3.5	3.5	4	4.5	4	3
25	6.5	6.5	7	6.5	6.5	6.5	6.5	6	6.5	6.5	7
26	6	4.5	5	5	3.5	5.5	5	1.5	2	4	5.5
27	4	4	4	4	4	4	4	4	4	4	4
28	5	5	6	5	5.5	3.5	5	4.5	4	4	5.5
29	4	6.5	2	6	6	6	6	4.5	4	5	5
30	1.5	2.5	1	3.5	3.5	3.5	3.5	3.5	2.5	3	3
31	5.5	5.5	5	6	4.5	4.5	6	3.5	3.5	3.5	4.5
32	1	4	2	1	4	3	1	1.5	4	3	4.5

Response ID	Field of Discipline	Org Position	Experience	Org	Incident Experience	Org Response Framework	NIST Familiarity	ICS/NIMS Familiarity	Common Terminology (AVG)	Integrated Comms (AVG)	Modular Org (AVG)	Command (AVG)	Span Control (AVG)
33	EM/HS	SL	≥5 yrs	GO	YR	Unknown	No	Yes	5.5	5.67	6	6.5	6
34	IT/CS	SL	≥5 yrs	GO	No	NIST	Yes	Yes	5.5	5.00	6	5	5
35	IT/CS	PR	≥5 yrs	GO	No	NIST	No	No	3	5.33	3	6	5.5
36	EM/HS	MM	≥5 yrs	GO	No	ICS/NIMS	No	Yes	6	6.00	6	6	6
37	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	7	6.33	7	7	4
38	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	6.5	7.00	6.5	7	6.5
39	EM/HS	MM	≥5 yrs	PS	YR	Both	No	Yes	4.5	5.00	5	5.5	3
40	IT/CS	PR	<5 yrs	GO	No	Both	Yes	Yes	6	5.67	6	6	4
41	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	4	4.33	3.5	5	5
42	EM/HS	MM	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	4	5.67	5.5	6.5	6
43	IT/CS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	4.5	3.33	4	5	3
44	EM/HS	MM	≥5 yrs	GO	YR	Other	Yes	Yes	5.5	5.33	5	5	3.5
45	EM/HS	PR	≥5 yrs	GO	YR	Other	No	Yes	4.5	5.00	4	4.5	3.5
46	EM/HS	PR	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	5	5.00	2.5	5	4.5
47	EM/HS	MM	<5 yrs	GO	No	ICS/NIMS	No	Yes	4	4.67	6	6.5	4.5
48	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	5	5.00	5.5	5.5	6
49	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	No	Yes	1.5	4.00	6	6	6
50	EM/HS	MM	≥5 yrs	GO	No	Unknown	No	Yes	1	1.67	1	3	3
51	EM/HS	MM	≥5 yrs	GO	No	ICS/NIMS	No	Yes	5	5.33	5	6	5.5
52	EM/HS	SL	≥5 yrs	GO	YR	ICS/NIMS	Yes	Yes	4	4.67	2	2	6
53	IT/CS	MM	≥5 yrs	PS	YR	Other	Yes	Yes	6	5.67	5	4	5
54	EM/HS	MM	<5 yrs	GO	No	Both	No	Yes	6.5	6.33	7	6.5	6.5
55	IT/CS	SL	≥5 yrs	PS	YR	Both	Yes	Yes	6	6.00	6.5	6.5	6
56	EM/HS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	6	6.00	6	6	6
57	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	4	3.33	4	4	3
58	IT/CS	SL	≥5 yrs	PS	YR	NIST	Yes	No	6	5.67	3.5	4	2.5
59	IT/CS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	4	7.00	6.5	6.5	1.5
60	IT/CS	PR	<5 yrs	GO	YR	Both	Yes	Yes	7	7.00	7	7	5.5
61	IT/CS	PR	<5 yrs	GO	YR	Both	Yes	Yes	5	6.00	6	6	6
62	EM/HS	MM	≥5 yrs	GO	No	ICS/NIMS	No	Yes	3	6.00	7	6.5	6
63	EM/HS	SL	≥5 yrs	GO	YR	Unknown	No	Yes	5	5.67	5	5.5	5.5
64	IT/CS	MM	≥5 yrs	GO	YR	Both	Yes	Yes	5.5	5.33	5	5.5	5.5
65	IT/CS	PR	≥5 yrs	GO	No	NIST	Yes	No	5	5.33	4	4	5

Response ID	Action Plans (AVG)	Resources (AVG)	Facilities (AVG)	Ext Common Terminology (AVG)	Ext Integrated Comms (AVG)	Ext Modular Org (AVG)	Ext Command (AVG)	Ext Span (AVG)	Ext Action Plans (AVG)	Ext Resources (AVG)	Ext Facilities (AVG)
33	6	4.5	6	5.5	5	6	5.5	5	5	4.5	5
34	2.5	5	5	5	4	5	5	3.5	4.5	4.5	4.5
35	5.5	5	6	5	4.5	4.5	5	4	4	4	4
36	6	6	5	4.5	3.5	4.5	4.5	4	4	4	4
37	6	6.5	7	5	3.5	4.5	5	4.5	4.5	3.5	4
38	6	6.5	3	4.5	4.5	5.5	4.5	4	2.5	4	3
39	4	5	6	4.5	5	5	4.5	4	3	4.5	5
40	5.5	5.5	5	5.5	3.5	5	5.5	4	4	4.5	4
41	5	6	5	4	4	4	4	4	4	4.5	4
42	6.5	6	3	5	6	4	5	6	2.5	2	3.5
43	3.5	5.5	5	5.5	3.5	4.5	5.5	4	3	4.5	4
44	4	4	5	5	4.5	5	5	4	4.5	4.5	5.5
45	4	4.5	5	4	4	4	4	4	3.5	4.5	4.5
46	4	4	1	4.5	4	3.5	4.5	3.5	3	4	4.5
47	5.5	7	7	5.5	2	3.5	5.5	2.5	4	3	4.5
48	5.5	6	4	4.5	4.5	5	4.5	4	4	4	4.5
49	4	6	2	2	4	2	2	6	4	2	4
50	1	3.5	1	4	3.5	3.5	4	4.5	4	3	4
51	6	6	6	5	4	5	5	4.5	4.5	4.5	4
52	4	4	6	4	4	4	4	4	3.5	4	4
53	5	5.5	4	6.5	3	3	6.5	3	2.5	3	2
54	7	6.5	7	3.5	5.5	4	3.5	5.5	3	6	6
55	6	6	6	4	5	5	4	4.5	5	4	5
56	5.5	6	6	4.5	4	3.5	4.5	4	3.5	3.5	3.5
57	3.5	3	5	4	3.5	3.5	4	4	3.5	4	3.5
58	2.5	2	6	6	4.5	2.5	6	2.5	2	3.5	3
59	6.5	3.5	6	2	3	3	2	4	5	1.5	3
60	5.5	7	7	5.5	6	5	5.5	5	5	4	4
61	6	6	6	5	5.5	6	5	4	6	4	5
62	6.5	6.5	7	4	4	6	4	2.5	3.5	2.5	5.5
63	5	5.5	6	5	5	4	5	4	4	4	5
64	5.5	6.5	6	4	4	4	4	4	4	4	4
65	4.5	5	6	5	5	3.5	5	4	3.5	4.5	5.5

Response ID	Field of Discipline	Org Position	Experience	Org	Incident Experience	Org Response Framework	NIST Familiarity	ICS/NIMS Familiarity	Common Terminology (AVG)	Integrated Comms (AVG)	Modular Org (AVG)	Command (AVG)	Span Control (AVG)
66	IT/CS	PR	<5 yrs	GO	YR	NIST	Yes	Yes	6.5	4.67	5.5	6	4.5
67	IT/CS	PR	≥5 yrs	GO	No	Both	No	No	2	5.00	4	4	6.5
68	IT/CS	PR	<5 yrs	GO	YR	Both	Yes	Yes	7	5.67	5.5	6	5.5
69	OT	PR	≥5 yrs	GO	No	Both	Yes	Yes	6	6.00	6	6	6.5
70	EM/HS	MM	≥5 yrs	GO	No	Unknown	No	Yes	4	4.00	4	4	4
71	EM/HS	MM	≥5 yrs	GO	No	Both	Yes	Yes	5.5	6.00	5.5	6	6
72	IT/CS	SL	≥5 yrs	GO	YR	Both	Yes	Yes	7	6.67	6	7	6.5
73	IT/CS	MM	≥5 yrs	PS	No	Both	Yes	Yes	5.5	3.67	5	4	5
74	IT/CS	SL	≥5 yrs	GO	No	Both	Yes	No	6	5.67	6	6	6
75	IT/CS	SL	≥5 yrs	GO	YR	Both	Yes	Yes	6	4.67	4	6	4
76	EM/HS	MM	≥5 yrs	GO	No	Both	No	Yes	7	7.00	7	7	7
77	IT/CS	SL	≥5 yrs	GO	No	NIST	Yes	Yes	5	4.67	6	4.5	2.5
78	IT/CS	MM	≥5 yrs	GO	YR	Other	Yes	Yes	2.5	2.67	3.5	2.5	3
79	IT/CS	PR	≥5 yrs	PS	YR	ICS/NIMS	Yes	No	6	5.67	4	5.5	4.5
80	EM/HS	SL	≥5 yrs	GO	No	ICS/NIMS	No	Yes	4	6.00	6	6	6
81	EM/HS	MM	≥5 yrs	GO	No	Both	No	Yes	6	6.00	6	5	4

Response ID	Action Plans (AVG)	Resources (AVG)	Facilities (AVG)	Ext Common Terminology (AVG)	Ext Integrated Comms (AVG)	Ext Modular Org (AVG)	Ext Command (AVG)	Ext Span (AVG)	Ext Action Plans (AVG)	Ext Resources (AVG)	Ext Facilities (AVG)
66	6	5	6	6	4.5	5	6	6	4	5	5
67	5.5	6.5	7	5.5	5	5.5	5.5	3.5	3.5	3.5	5
68	5.5	5	5	5.5	4.5	4.5	5.5	4	4.5	3.5	5
69	6	6	6	6	6	6	6	6	6	6	6
70	4	4	4	5.5	3.5	5	5.5	4	4.5	6	3.5
71	5.5	6.5	6	4.5	3.5	3.5	4.5	4	3.5	4	4.5
72	6.5	6.5	4	5.5	5	5	5.5	4.5	3	5.5	4.5
73	5	4.5	2	5.5	3	4.5	5.5	6	4	4.5	6
74	5.5	6	6	4	5	5	4	3.5	4	4	4.5
75	4	4	5	4	6	6	4	3	4	6	4
76	7	7	7	6.5	4.5	6.5	6.5	5	4	4	4.5
77	4	4	4	3	5.5	4	3	4	4	4	4.5
78	2.5	4	2	5	4.5	3.5	5	3.5	4.5	5.5	5
79	4	5.5	6	5	5.5	5	5	3.5	4	4	4.5
80	6	6	6	4	4	4	4	4	4	4	4
81	4	5	6	6	6	5	6	4	5	5	5

LIST OF REFERENCES

Allen, David. “Ransomware Incident Command & Lessons Learned for Managers.” Secure World Atlanta, August 2020.

Auf der Heide, Erik. *Disaster Response: Principles of Preparation and Coordination*. St. Louis, MO: Mosby, 1989.

Bennett, Brian. “Effective Emergency Management: A Closer Look at the Incident Command System.” *Professional Safety* 56, no. 11 (November 2011): 28–37. ProQuest.

Bigley, Gregory, and Karlene Roberts. “The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments.” *Academy of Management Journal* 44, no. 6 (2001): 1281–99.

Bismarck State College, College Relations. *Key Takeaways from the 2018 Ransomware Attack on Colorado DOT*. Video, 2019. https://vimeo.com/369910099.

Boylan, Amelia A., Audrey N. Tepe, and Danny W. Davis. “After the Ransomware Attacks: Texas Governance and Authorities for Cyberattack Response.” Homeland Security Today, November 13, 2019. https://www.hstoday.us/subject-matter-areas/infrastructure-security/after-the-ransomware-attacks-texas-governance-and-authorities-for-cyberattack-response/.

Buck, Dick A., Joseph E. Trainor, and Benigno E. Aguirre. “A Critical Evaluation of the Incident Command System and NIMS.” *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006). https://doi.org/10.2202/1547-7355.1252.

Burgiel, Stanley W. “The Incident Command System: A Framework for Rapid Response to Biological Invasion.” *Biological Invasions* 22, no. 1 (2020): 155–65. https://doi.org/10.1007/s10530-019-02150-2.

Cerulus, Laurens. “How Ukraine Became a Test Bed for Cyberweaponry.” Politico, February 14, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

Christen, Hank, Paul Maniscalco, Alan Vickery, and Frances Winslow. “An Overview of Incident Management Systems.” *Perspectives on Preparedness*, no. 4 (2001).

Coats, Daniel R. *Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Colorado Department of Transportation. *CDOT Cyber Incident: After-Action Report*. Denver: Colorado Department of Transportation, 2018. https://www.colorado.gov/pacific/dhsem/atom/129636.

Danko, Tiffany. “Student Perceptions in Homeland Security and Emergency Management Education: Experiential Learning Survey.” *Journal of Experiential Education* 42, no. 4 (2019): 417–27. https://doi.org/10.1177/1053825919873678.

Department of Health and Human Services. “Overview of MSCC, Emergency Management and the Incident Command System.” In *Medical Surge Capacity Handbook: A Management System for Integrating Medical and Health Resources During Large-Scale Emergencies*, 2nd ed. Washington, DC: Department of Health and Human Services, 2007. https://www.phe.gov/Preparedness/planning/mscc/handbook/chapter1/Pages/emergencymanagement.aspx.

Dixon, Herbert. “Cyberattacks on Courts and Other Government Institutions.” *Judges’ Journal* 57, no. 3 (Summer 2018): 37–39. ProQuest.

Emergency Management Institute. “Professional Development Series (PDS) Courses.” Independent Study Program (IS). Accessed January 28, 2021. https://training.fema.gov/is/searchis.aspx?search=PDS.

Federal Emergency Management Agency. *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101*. Washington, DC: Department of Homeland Security, 2010. https://www.ready.gov/sites/default/files/2019-06/comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans.pdf.

———. *National Incident Management System*. 3rd ed. Washington, DC: Department of Homeland Security, 2017. https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

———. “NIMS and the Incident Command System.” Washington, DC: Federal Emergency Management Agency, November 23, 2004. https://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

Freed, Benjamin. “How Texas Used Its Disaster Playbook after a Huge Ransomware Attack.” StateScoop, October 15, 2019. https://statescoop.com/texas-ransomware-emergency-declaration-nascio-19/.

———. “Indictments in Ransomware Spree on Cities, Agencies.” StateScoop, November 28, 2018. https://statescoop.com/ransomware-spree-against-atlanta-newark-and-others-leads-to-indictment-of-2-iranians/.

———. “What Colorado Learned from Treating a Cyberattack Like a Disaster.” StateScoop, May 15, 2019. https://statescoop.com/what-colorado-learned-from-treating-a-cyberattack-like-a-disaster/.

Givens, Austen. “Strengthening Cyber Incident Response Capabilities through Education and Training in the Incident Command System.” *National Cybersecurity Institute Journal* 2, no. 3 (2015): 65–75. http://publications.excelsior.edu/publications/NCI_Journal/2-3/nci-journal-vol-2-no-3.pdf#page=67.

Hannestad, Stephen E. “Incident Command System: A Developing National Standard of Incident Management in the U.S.” In *Proceedings of the 2nd International ISCRAM Conference*, edited by B. Van de Walle and B. Carlé, 19–28. Brussels: Information Systems for Crisis Response and Management, 2005. http://idl.iscram.org/files/hannestad/2005/559_Hannestad2005.pdf.

Harrald, John R. “Agility and Discipline: Critical Success Factors for Disaster Response.” *Annals of the American Academy of Political and Social Science* 604, no. 1 (2006): 256–72. https://doi.org/10.1177/0002716205285404.

Jensen, Jessica, and Steven Thompson. “The Incident Command System: A Literature Review.” *Disasters* 40, no. 1 (January 2016): 158–82. https://doi.org/10.1111/disa.12135.

Larence, Eileen R. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors’ Characteristics*. GAO-07-39. Washington, DC: Government Accountability Office, 2006. https://www.gao.gov/assets/260/252603.pdf.

Lester, William, and Daniel Krejci. “Business ‘Not’ as Usual: The National Incident Management System, Federalism, and Leadership.” *Public Administration Review* 67 (2007): 84–93. https://doi.org/10.1111/j.1540-6210.2007.00817.x.

McLoughlin, Emily Jane. “Beyond the First 48: Incorporating Nontraditional Stakeholders into Incident Response.” Master’s thesis, Naval Postgraduate School, 2020. http://hdl.handle.net/10945/66108.

Moore, Erik L., Steven P. Fulton, Roberta A. Mancuso, Tristen K. Amador, and Daniel M. Likarish. “Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation.” In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, 1–8. Oxford, UK: IEEE, 2019. https://doi.org/10.1109/CyberSA.2019.8899736.

Morris, Charles. *Using the FEMA Incident Command System to Manage Computer Security Incidents*. Bethesda, MD: SANS Institute, 2004. https://www.giac.org/paper/gsec/4037/fema-incident-command-system-manage-computer-security-incidents/106431.

Moynihan, D. P. "The Network Governance of Crisis Response: Case Studies of Incident Command Systems." *Journal of Public Administration Research and Theory* 19, no. 4 (2009): 895–915. https://doi.org/10.1093/jopart/mun033.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, DC: The National Commission on Terrorist Attacks Upon the United States, 2004. https://govinfo.library.unt.edu/911/report/911Report.pdf.

ND Dept of Emergency Management IT Department. *Michael Willis*. Video, 2019. https://www.youtube.com/watch?v=7gkDAHqO-24&feature=youtu.be.

Perry, Ronald W. "Incident Management Systems in Disaster Management." *Disaster Prevention and Management: An International Journal* 12, no. 5 (2003): 405–12. https://doi.org/10.1108/09653560310507226.

State of Louisiana. "State of Emergency - Cybersecurity Incident." Baton Rouge: State of Louisiana, July 24, 2019. https://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf.

Texas Cybersecurity Update. Video, 2020. https://www.youtube.com/watch?v=N9jhrrvf7zM.

Texas Department of Information Resources. "August Incident Hotwash #1 Outcomes." Austin, TX: Texas Department of Information Resources, n.d. Accessed March 20, 2020.

———. *Incident Response Team Redbook*. Austin, TX: Texas Department of Information Resources, 2020. https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template.pdf.

———. "Ransomware and Incident Response in Texas." Austin, TX: Office of the Chief Information Officer, Texas Department of Information Resources, January 2020.

U.S. Department of Homeland Security. *National Cyber Incident Response Plan*. Washington, DC: Department of Homeland Security, 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

———. *National Incident Management System*. Washington, DC: Department of Homeland Security, 2008. https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

———. *The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO)Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP)*. Washington, DC: Department of Homeland Security, 2020. https://www.fema.gov/sites/default/files/2020-08/fema_homeland-security-grant-program-nofo_fy-2020.pdf.

U.S. Department of Justice. “Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses.” Justice News, November 28, 2018. https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

Waugh, William L., and Gregory Streib. “Collaboration and Leadership for Effective Emergency Management.” *Public Administration Review* 66 (2006): 131–40. https://doi.org/10.1111/j.1540-6210.2006.00673.x.

Wise, Charles R. “Organizing for Homeland Security after Katrina: Is Adaptive Management What’s Missing?” *Public Administration Review* 66, no. 3 (2006): 302–18. https://doi.org/10.1111/j.1540-6210.2006.00587.x.

Zach. “What Is Considered to Be a ‘Strong’ Correlation?” *Statology* (blog), January 22, 2020. https://www.statology.org/what-is-a-strong-correlation/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California